(2)

明 特2

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-179592
(43)Date of publication of application : 27.06.2003

(51)Int.Cl. H04L 9/08

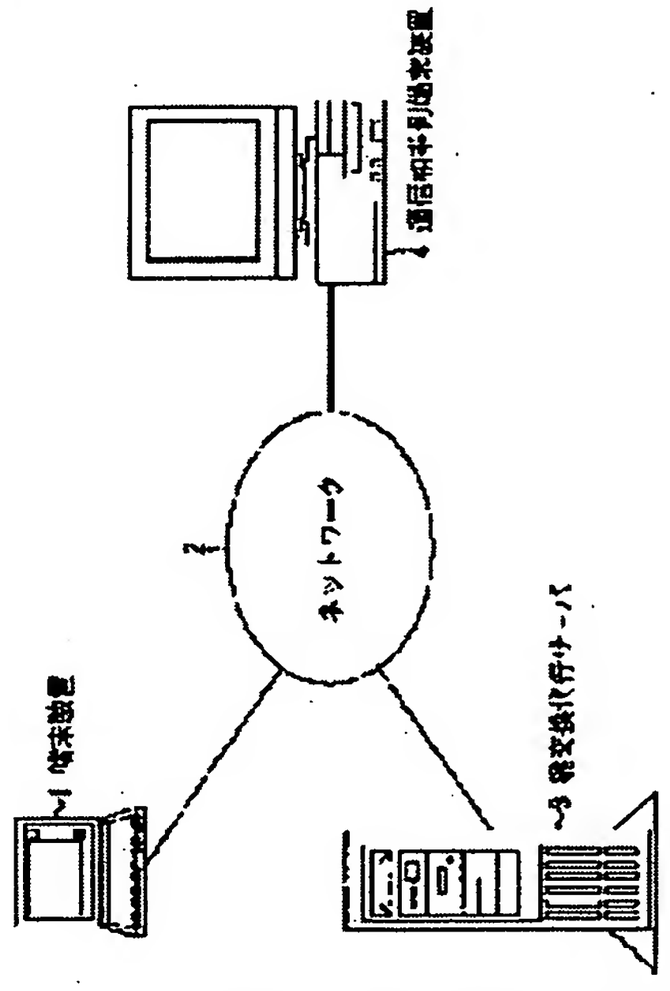
(21)Application number : 2001-378413
(22)Date of filing : 12.12.2001

(71)Applicant : SONY CORP
(72)Inventor : HAMANO JUNJI

(54) NETWORK SYSTEM, DEVICE AND METHOD FOR PROCESSING INFORMATION, RECORDING MEDIUM AND PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To reduce a burden caused by key exchange processing in an information processor to perform a communication, and to enable even equipment limited in calculation resources to exchange a key while keeping compatibility with existent key exchange protocol.
SOLUTION: A terminal device 1 is connected to a network 2 representatively such as the Internet and performs the cipher communication of enciphered communication contents with a communicating party terminal device 4 via the network 2 by IPsec, SSL or TSL. A key exchange substitution server 3 is connected to the network and substitutes various kinds of processing such as processing for determining the cipher algorithm or key exchange method of key exchange processing to be performed by the terminal device 1 while using IKE or TLS handshake protocol in order to share a common key with the communication party terminal device 4, key generating processing and authentic processing.

図1



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

特2.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－179592
（P2003－179592A）
(43)公開日　平成15年６月27日(2003.6.27)

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ　５Ｊ１０４
			６０１Ｅ
			６０１Ｃ

審査請求　未請求　請求項の数16　ＯＬ　（全 19 頁）

(21)出願番号　特願2001－378413(P2001－378413)

(22)出願日　平成13年12月12日(2001.12.12)

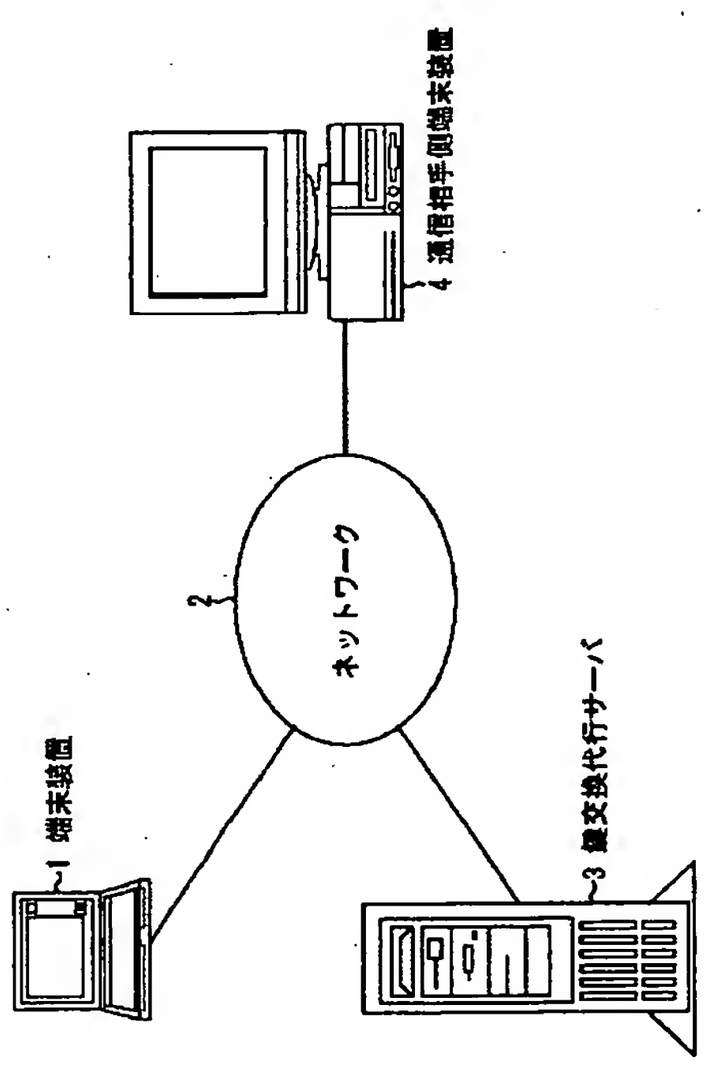
(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　濱野　淳史
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082131
弁理士　稲本　義雄

Ｆターム(参考)　5J104 DA03 EA04 EA18 JA03 NA02 NA03 PA07

(54)【発明の名称】　ネットワークシステム、情報処理装置および方法、記録媒体、並びにプログラム

(57)【要約】
【課題】　通信を行う情報処理装置の鍵交換処理による負担を軽減し、計算資源が限られた機器においても、既存の鍵交換プロトコルとの互換性を保ちつつ鍵交換を実現することができるようにする。
【解決手段】　端末装置１は、インターネット等に代表されるネットワーク２に接続されており、ネットワーク２を介して、IPsec，SSL、またはTSL等により、通信相手側端末装置４と通信内容が暗号化された暗号通信を行う。鍵交換代行サーバ３は、ネットワーク２に接続されており、端末装置１が通信相手端末装置４と共通鍵を共有するために、IKEやTLS Handshake Protocolを用いて行う鍵交換処理の暗号化アルゴリズムや鍵交換方法を決定する処理、鍵生成処理、および認証処理等の各種処理を代行する。

図1



【特許請求の範囲】
【請求項１】　ネットワークに接続され、他の情報処理装置と暗号通信を行う第１の情報処理装置と、
前記ネットワークに接続され、前記第１の情報処理装置が前記暗号通信に用いる共通鍵を、通信相手である前記他の情報処理装置と共有するための、前記第１の情報処理装置による鍵交換処理を代行する第２の情報処理装置とを備えるネットワークシステムであって、
前記第１の情報処理装置は、
前記他の情報処理装置と前記暗号通信を行う暗号通信手段と、
前記鍵交換処理の代行を要求する要求メッセージを前記第２の情報処理装置に供給する要求メッセージ供給手段と、
前記要求メッセージ供給手段により供給された前記要求メッセージに対応する応答メッセージを、前記第２の情報処理装置より取得する応答メッセージ取得手段と、
前記応答メッセージ取得手段により取得された前記応答メッセージに基づいて、前記暗号通信に用いるセッションごとの前記共通鍵であるセッション鍵を設定するセッション鍵設定手段とを備え、
前記第２の情報処理装置は、
前記要求メッセージを前記第１の情報処理装置より取得する要求メッセージ取得手段と、
前記要求メッセージ取得手段により取得された前記要求メッセージに基づいて、前記鍵交換処理を代行して行う鍵交換代行処理手段と、
前記鍵交換代行処理手段の処理結果に基づいて、前記要求メッセージに対応する前記応答メッセージを、前記第１の情報処理装置に供給する応答メッセージ供給手段とを備えることを特徴とするネットワークシステム。
【請求項２】　前記要求メッセージは、
前記鍵交換処理の開始を示し、鍵交換方法の決定を要求する開始要求メッセージと、
前記共通鍵の生成を要求する鍵生成要求メッセージと、
前記第１の情報処理装置の通信相手である前記他の情報処理装置の認証を要求する認証要求メッセージと、
前記セッション鍵を要求する鍵要求メッセージとを含み、
前記応答メッセージは、
前記開始要求メッセージに対応する開始応答メッセージと、
前記鍵生成要求メッセージに対応する鍵生成応答メッセージと、
前記認証要求メッセージに対応する認証応答メッセージと、
前記鍵要求メッセージに対応する鍵応答メッセージとを含み、
前記鍵交換代行処理手段は、
前記開始要求メッセージに基づいて、前記暗号通信における鍵交換方法を決定する鍵交換方法決定手段と、

前記鍵生成要求メッセージに基づいて、前記共通鍵を生成する共通鍵生成手段と、
前記認証要求メッセージに基づいて、前記第１の情報処理装置の通信相手である前記他の情報処理装置を認証する認証手段と、
前記認証要求メッセージに基づいて、前記第１の情報処理装置の通信相手である前記他の情報処理装置が前記第１の情報処理装置にアクセス可能か否かを確認する確認手段と、
前記鍵要求メッセージに基づいて、前記セッション鍵に関する処理を行うセッション鍵処理手段とを備えることを特徴とする請求項１に記載のネットワークシステム。
【請求項３】　前記鍵交換方法は、IKE、または、SSL若しくはTLSのHandshake Protocolを含むことを特徴とする請求項２に記載のネットワークシステム。
【請求項４】　前記第１の情報処理装置は、
前記第２の情報処理装置と安全に通信が行えるか否かを判定する第１の判定手段と、
前記第１の判定手段の判定結果に基づいて、前記第２の情報処理装置と安全に通信するための、前記第２の情報処理装置と共有する共通鍵を設定する第１の共通鍵設定手段とをさらに備え、
前記第２の情報処理装置は、
前記第１の情報処理装置と安全に通信が行えるか否かを判定する第２の判定手段と、
前記第２の判定手段の判定結果に基づいて、前記第１の情報処理装置と安全に通信するための、前記第１の情報処理装置と共有する共通鍵を設定する第２の共通鍵設定手段とをさらに備えることを特徴とする請求項１に記載のネットワークシステム。
【請求項５】　ネットワークに接続され、第１の他の情報処理装置と暗号通信を行う情報処理装置であって、
前記第１の他の情報処理装置と暗号通信を行う暗号通信手段と、
前記暗号通信手段による前記暗号通信に用いる共通鍵を記憶する記憶手段と、
前記共通鍵を前記第１の他の情報処理装置と共有するための鍵交換処理の代行を要求する要求メッセージを、前記鍵交換処理を代行する第２の他の情報処理装置に供給する要求メッセージ供給手段と、
前記要求メッセージ供給手段により供給された要求メッセージに対応する応答メッセージを、前記第２の他の情報処理装置より取得する応答メッセージ取得手段と、
前記応答メッセージ取得手段により取得された前記応答メッセージに基づいて、前記暗号通信のセッションごとの前記共通鍵であるセッション鍵を設定するセッション鍵設定手段とを備えることを特徴とする情報処理装置。
【請求項６】　前記第２の他の情報処理装置と安全に通信が行えるか否かを判定する判定手段と、

前記判定手段の判定結果に基づいて、前記第２の他の情報処理装置と安全に通信するための、前記第２の他の情報処理装置と共有する共通鍵を設定する共通鍵設定手段とをさらに備えることを特徴とする請求項５に記載の情報処理装置。

【請求項７】　暗号通信に用いる共通鍵を記憶する記憶部を有し、ネットワークに接続され、第１の他の情報処理装置と暗号通信を行う情報処理装置の情報処理方法であって、

前記第１の他の情報処理装置と前記暗号通信を行う暗号通信ステップと、

前記暗号通信ステップの処理による前記暗号通信に用いる共通鍵の記憶部からの取得を制御する記憶制御ステップと、

前記暗号通信ステップの処理による前記暗号通信に用いる共通鍵を前記第１の他の情報処理装置と共有するための鍵交換処理の代行を要求する要求メッセージを、前記鍵交換処理を代行する第２の他の情報処理装置に供給する要求メッセージ供給ステップと、

前記要求メッセージ供給ステップの処理により供給された要求メッセージに対応する応答メッセージの、前記第２の他の情報処理装置からの取得を制御する応答メッセージ取得制御ステップと、

前記応答メッセージ取得制御ステップの処理により取得が制御された前記応答メッセージに基づいて、前記暗号通信のセッションごとの前記共通鍵であるセッション鍵を設定するセッション鍵設定ステップとを含むことを特徴とする情報処理方法。

【請求項８】　暗号通信に用いる共通鍵を記憶する記憶部を有し、ネットワークに接続され、第１の他の情報処理装置と前記暗号通信を行う情報処理装置用のプログラムであって、

前記第１の他の情報処理装置と前記暗号通信を行う暗号通信ステップと、

前記暗号通信ステップの処理による前記暗号通信に用いる共通鍵の記憶部からの取得を制御する記憶制御ステップと、

前記暗号通信ステップの処理による前記暗号通信に用いる共通鍵を前記第１の他の情報処理装置と共有するための鍵交換処理の代行を要求する要求メッセージを、前記鍵交換処理を代行する第２の他の情報処理装置に供給する要求メッセージ供給ステップと、

前記要求メッセージ供給ステップの処理により供給された要求メッセージに対応する応答メッセージの、前記第２の他の情報処理装置からの取得を制御する応答メッセージ取得制御ステップと、

前記応答メッセージ取得制御ステップの処理により取得が制御された前記応答メッセージに基づいて、前記暗号通信のセッションごとの前記共通鍵であるセッション鍵を設定するセッション鍵設定ステップとを含むことを特

徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項９】　暗号通信に用いる共通鍵を記憶する記憶部を有し、ネットワークに接続され、第１の他の情報処理装置と前記暗号通信を行う情報処理装置を制御するコンピュータが実行可能なプログラムであって、

前記第１の他の情報処理装置と前記暗号通信を行う暗号通信ステップと、

前記暗号通信ステップの処理による前記暗号通信に用いる共通鍵の記憶部からの取得を制御する記憶制御ステップと、

前記暗号通信ステップの処理による前記暗号通信に用いる共通鍵を前記第１の他の情報処理装置と共有するための鍵交換処理の代行を要求する要求メッセージを、前記鍵交換処理を代行する第２の他の情報処理装置に供給する要求メッセージ供給ステップと、

前記要求メッセージ供給ステップの処理により供給された要求メッセージに対応する応答メッセージの、前記第２の他の情報処理装置からの取得を制御する応答メッセージ取得制御ステップと、

前記応答メッセージ取得制御ステップの処理により取得が制御された前記応答メッセージに基づいて、前記暗号通信のセッションごとの前記共通鍵であるセッション鍵を設定するセッション鍵設定ステップとを含むことを特徴とするプログラム。

【請求項１０】　ネットワークに接続され、第１の他の情報処理装置が、前記第１の他の情報処理装置により行われる暗号通信に用いられる共通鍵を、通信相手である第２の他の情報処理装置と共有するための、前記第１の他の情報処理装置による鍵交換処理を代行する情報処理装置であって、

前記鍵交換処理に関する情報を記憶する記憶手段と、

前記鍵交換処理の代行を要求する要求メッセージを、前記第１の他の情報処理装置より取得する要求メッセージ取得手段と、

前記要求メッセージ取得手段により取得された前記要求メッセージに基づいて、前記鍵交換処理を代行して行う鍵交換代行処理手段と、

前記鍵交換代行処理手段の処理結果に基づいて、前記要求メッセージに対応する前記応答メッセージを、前記第１の他の情報処理装置に供給する応答メッセージ供給手段とを備えることを特徴とする情報処理装置。

【請求項１１】　前記要求メッセージは、

前記鍵交換処理の開始を示し、鍵交換方法の決定を要求する開始要求メッセージと、

前記共通鍵の生成を要求する鍵生成要求メッセージと、

前記第２の他の情報処理装置の認証を要求する認証要求メッセージと、

前記暗号通信のセッションごとの前記共通鍵であるセッション鍵を要求する鍵要求メッセージとを含み、

前記応答メッセージは、
前記開始要求メッセージに対応する開始応答メッセージと、
前記鍵生成要求メッセージに対応する鍵生成応答メッセージと、
前記認証要求メッセージに対応する認証応答メッセージと、
前記鍵要求メッセージに対応する鍵応答メッセージとを含み、
前記鍵交換代行処理手段は、
前記開始要求メッセージに基づいて、前記暗号通信における鍵交換方法を決定する鍵交換方法決定手段と、
前記鍵生成要求メッセージに基づいて、前記共通鍵を生成する共通鍵生成手段と、
前記認証要求メッセージに基づいて、前記第２の他の情報処理装置を認証する認証手段と、
前記認証要求メッセージに基づいて、前記第２の他の情報処理装置が前記第１の他の情報処理装置にアクセス可能か否かを確認する確認手段と、
前記鍵要求メッセージに基づいて、前記セッション鍵に関する処理を行うセッション鍵処理手段とを備えることを特徴とする請求項１０に記載の情報処理装置。
【請求項１２】　前記第２の情報処理装置は、
前記第１の他の情報処理装置と安全に通信が行えるか否かを判定する判定手段と、
前記判定手段の判定結果に基づいて、前記第１の他の情報処理装置と安全に通信するための、前記第１の他の情報処理装置と共有する共通鍵を設定する共通鍵設定手段とをさらに備えることを特徴とする請求項１０に記載の情報処理装置。
【請求項１３】　前記記憶手段により記憶されている前記鍵交換処理に関する情報は、前記第２の他の情報処理装置の認証に関する情報、および前記第２の他の情報処理装置が前記第１の他の情報処理装置にアクセス可能か否かに関する情報であるポリシ情報を含むことを特徴とする請求項１０に記載の情報処理装置。
【請求項１４】　前記鍵交換処理に関する情報を記憶する記憶部を有し、ネットワークに接続され、第１の他の情報処理装置が、前記第１の他の情報処理装置により行われる暗号通信に用いられる共通鍵を、通信相手である第２の他の情報処理装置と共有するための、前記第１の他の情報処理装置による鍵交換処理を代行する情報処理装置の情報処理方法であって、
前記鍵交換処理に関する情報の記憶部からの取得を制御する記憶制御ステップと、
前記鍵交換処理の代行を要求する要求メッセージの、前記第１の他の情報処理装置からの取得を制御する要求メッセージ取得制御ステップと、
前記要求メッセージ取得制御ステップの処理により取得が制御された前記要求メッセージに基づいて、前記鍵交

換処理を代行して行う鍵交換代行処理ステップと、
前記鍵交換代行処理ステップの処理の処理結果に基づいて、前記要求メッセージに対応する前記応答メッセージを、前記第１の他の情報処理装置に供給する応答メッセージ供給ステップとを備えることを特徴とする情報処理方法。
【請求項１５】　前記鍵交換処理に関する情報を記憶する記憶部を有し、ネットワークに接続され、第１の他の情報処理装置が、前記第１の他の情報処理装置により行われる暗号通信に用いられる共通鍵を、通信相手である第２の他の情報処理装置と共有するための、前記第１の他の情報処理装置による鍵交換処理を代行する情報処理装置用のプログラムであって、
前記鍵交換処理に関する情報の記憶部からの取得を制御する記憶制御ステップと、
前記鍵交換処理の代行を要求する要求メッセージの、前記第１の他の情報処理装置からの取得を制御する要求メッセージ取得制御ステップと、
前記要求メッセージ取得制御ステップの処理により取得が制御された前記要求メッセージに基づいて、前記鍵交換処理を代行して行う鍵交換代行処理ステップと、
前記鍵交換代行処理ステップの処理の処理結果に基づいて、前記要求メッセージに対応する前記応答メッセージを、前記第１の他の情報処理装置に供給する応答メッセージ供給ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。
【請求項１６】　前記鍵交換処理に関する情報を記憶する記憶部を有し、ネットワークに接続され、第１の他の情報処理装置が、前記第１の他の情報処理装置により行われる暗号通信に用いられる共通鍵を、通信相手である第２の他の情報処理装置と共有するための、前記第１の他の情報処理装置による鍵交換処理を代行する情報処理装置を制御するコンピュータが実行可能なプログラムであって、
前記鍵交換処理に関する情報の記憶部からの取得を制御する記憶制御ステップと、
前記鍵交換処理の代行を要求する要求メッセージの、前記第１の他の情報処理装置からの取得を制御する要求メッセージ取得制御ステップと、
前記要求メッセージ取得制御ステップの処理により取得が制御された前記要求メッセージに基づいて、前記鍵交換処理を代行して行う鍵交換代行処理ステップと、
前記鍵交換代行処理ステップの処理の処理結果に基づいて、前記要求メッセージに対応する前記応答メッセージを、前記第１の他の情報処理装置に供給する応答メッセージ供給ステップとを含むことを特徴とするプログラム。
【発明の詳細な説明】
【０００１】

【発明の属する技術分野】本発明はネットワークシステム、情報処理装置および方法、記録媒体、並びにプログラムに関し、特に、暗号通信における鍵交換処理を代行することにより、通信を行う情報処理装置の負担を軽減するネットワークシステム、情報処理装置および方法、記録媒体、並びにプログラムに関する。

【０００２】

【従来の技術】近年、インターネットに代表されるネットワークの普及とともに、電子メールやファイルの送受信がさかんに行われるようになってきた。それに伴い、セキュリティに対する不安も多くなっている。

【０００３】従来、インターネット等のネットワークにおいて利用されるセキュリティ機構としては、RFC（Request For Comment）２４０１に規定されているIP（InternetProtocol）層でのセキュリティ機構であるIPsec（Internet Protocol securityarchitecture）、WEBで利用されるSSL（Secure Socket Layer）、および、その後継技術でありRFC２２４６に規定されているTLS（Transport Layer Security）等がある。

【０００４】これらのプロトコルでは、安全な通信を行う前に、通信者間で暗号通信に利用されるセッション鍵を共有する必要がある。その方法としては、RFC２４０９で規定されているIKE（Internet Key Exchange）、または、SSLやTLSに含まれるHandshake Protocol等がある。

【０００５】IKEは、IPsecに必要な鍵を動的に確立する独立した機構であり、RFC２４０７およびRFC２４０８に規定されている、鍵交換の枠組みを提供するISAKMP（Internet Security Association and Key Management Protocol）と、ISAKMP上で実際の鍵管理機構を定義しているOakleyからなる。

【０００６】IKEは、ISAKMPのためのISAKMP SA（ISAKMP Security Association）を確立するPhase１と、IPsecのSAを確立するPhase２により構成される。なお、SAとは、通信を保護するために用いられる方針や鍵の集合のことである。Phase１には通信者のIDの保護が可能なメインモードと、IDの保護が不可能なアグレッシブモードの２つが存在し、Phase２にはクイックモードのみが存在する。

【０００７】メインモードでは、始動者と応答者の間で、６回（３往復）の通信を行ってISAKMPを確立する。始めの２回（１往復）の通信において両者で使用するアルゴリズム等の取り決めが行われ、次の２回（１往復）の通信において鍵交換に必要なDiffie-Hellman鍵交換アルゴリズムの公開値や乱数等の補助的なデータの交換が行われる。そして、最後の２回（１往復）の通信で生成された鍵の認証が行われる。

【０００８】これに対して、アグレッシブモードでは、始動者と応答者の間で、３回（１．５往復）の通信を行い、ISAKMP SAを確立する。始めの２回（１往復）の通信において両者で使用するアルゴリズム等の取り決めと、鍵交換に必要なDiffie-Hellman鍵交換アルゴリズムの公開値や乱数等の補助的なデータの交換が行われる。そして、３回目の通信において、始動者の認証と生成された鍵の認証が行われる。この３回目の通信は、生成されるISAKMP SAによって暗号化されない。従って、IDの保護が不可能となる。

【０００９】メインモード、アグレッシブモードにおいては、電子署名、公開鍵暗号、予め保持している共通鍵を用いる方法の３種類の認証方法が利用可能である。

【００１０】Phase２のクイックモードにおいては、始動者と応答者の間で、３回（１．５往復）の通信を行い、IPsecのSAを確立する。クイックモードにおける通信内容は、ISAKMP SAによって保護される。始めの２回（１往復）の通信において、両者で使用するアルゴリズム等の取り決めが行われ、３回目の通信で生成された鍵の認証が行われる。

【００１１】以上のようにして、IPsecで安全な通信を行う前に通信者間で暗号通信に利用されるセッション鍵を共有することができる。

【００１２】また、TLSは、クライアントーサーバアプリケーションに対してセキュリティを提供するプロトコルであり、鍵交換についてはHandshake Protocolとして規定されている。Handshake Protocolによるクライアントーサーバ間の処理は、以下のように行われる。

【００１３】最初に、クライアントは、ClientHelloメッセージを用いて、クライアントで利用可能な暗号化アルゴリズムに関する情報をサーバに供給する。サーバは、その中から使用する暗号化アルゴリズムを選択し、その暗号化アルゴリズムに関する情報を、ServerHelloメッセージを用いてクライアントに供給する。また、サーバは、ServerHelloメッセージを送信した後に、ServerCertificateメッセージを用いてサーバ自身の証明書を送信する。サーバの証明書が存在しない場合、サーバは、合意過程で使用する仮の暗号化鍵等を送信するServerKeyExchangeメッセージをクライアントに送信する。さらに、サーバは、必要であれば、クライアントの証明書の送付を要求するCertificateReqestメッセージも送信する。そして、サーバは、ServerHelloDoneメッセージを送信することによってサーバからの送信を終了し、クライアントからの返答を待つ。

【００１４】サーバからCertificateReqestメッセージを送信されたクライアントは、ClientCertificateメッセージによりクライアントの証明書を送信する。そして、証明書を送信したクライアントは、セッション鍵生成の元となるpre-master keyをサーバの公開鍵で暗号化し、その暗号化されたpre-master key を含むClientKeyExchangeメッセージをサーバに送信する。

【００１５】また、クライアントは、ClientHelloメッセージから直前までの通信内容のダイジェストをクライ

アントの秘密鍵で暗号化して、CertificateVerifyメッセージに含めてサーバに送信する。サーバは、それを公開鍵で複合化して、クライアント証明書の正当性を確認する。

【００１６】この時点で、セッション鍵などが利用可能となっており、クライアントは、暗号仕様の変更を合図するChangeCipherSpecメッセージを送信した後に、セッション鍵などを設定する。これにより、これ以降の通信は、設定されたセッション鍵を利用して、Helloメッセージで決定したアルゴリズムにより守られるようになる。最後にクライアントは、Finishedメッセージを送信し、終了する。また、サーバにおいても、上述したクライアントの場合と同様に、ChangeCipherSpecメッセージを送信し、セッション鍵などを設定し、Finishedメッセージを送信する。

【００１７】以上のようにして、クライアントーサーバ間において、安全な通信を行うためのセッション鍵を共有することができる。

【００１８】

【発明が解決しようとする課題】しかしながら、以上のような方法の場合、公開鍵暗号アルゴリズムを利用した認証処理やDiffie-Hellman鍵交換アルゴリズムの計算処理等の負荷の大きな処理が必要であり、計算資源が限られた機器等において、その処理に多大な時間を要する場合があるという課題があった。

【００１９】また、特開２００１－１９７０５５号公報には、機能の乏しい携帯端末であっても、認証局で認証を得た証明書を用いた情報通信を行うことができ、ユーザ等が、複数の認証局が発行した証明書の検証や管理等に対する作業負荷を軽減することが可能な認証代行装置が開示されているが、認証処理の代行のみが目的であり、安全な通信を実現するための鍵の交換方法については提供されていないという課題があった。

【００２０】さらに、この場合、ユーザ端末とサーバとの間に認証代行サーバが介在するので、既存の通信プロトコルと互換性を保つことができないという課題もあった。

【００２１】本発明はこのような状況に鑑みてなされたものであり、暗号通信における鍵交換処理を代行することにより、通信を行う情報処理装置の負担を軽減することができるようにしたものである。

【００２２】

【課題を解決するための手段】本発明のネットワークシステムは、ネットワークに接続され、他の情報処理装置と暗号通信を行う第１の情報処理装置と、ネットワークに接続され、第１の情報処理装置が暗号通信に用いる共通鍵を、通信相手である他の情報処理装置と共有するための、第１の情報処理装置による鍵交換処理を代行する第２の情報処理装置とを備えるネットワークシステムであって、第１の情報処理装置は、他の情報処理装置と暗

号通信を行う暗号通信手段と、鍵交換処理の代行を要求する要求メッセージを第２の情報処理装置に供給する要求メッセージ供給手段と、要求メッセージ供給手段により供給された要求メッセージに対応する応答メッセージを、第２の情報処理装置より取得する応答メッセージ取得手段と、応答メッセージ取得手段により取得された応答メッセージに基づいて、暗号通信に用いるセッションごとの共通鍵であるセッション鍵を設定するセッション鍵設定手段とを備え、第２の情報処理装置は、要求メッセージを第１の情報処理装置より取得する要求メッセージ取得手段と、要求メッセージ取得手段により取得された要求メッセージに基づいて、鍵交換処理を代行して行う鍵交換代行処理手段と、鍵交換代行処理手段の処理結果に基づいて、要求メッセージに対応する応答メッセージを、第１の情報処理装置に供給する応答メッセージ供給手段とを備えることを特徴とする。

【００２３】前記要求メッセージは、鍵交換処理の開始を示し、鍵交換方法の決定を要求する開始要求メッセージと、共通鍵の生成を要求する鍵生成要求メッセージと、第１の情報処理装置の通信相手である他の情報処理装置の認証を要求する認証要求メッセージと、セッション鍵を要求する鍵要求メッセージとを含み、応答メッセージは、開始要求メッセージに対応する開始応答メッセージと、鍵生成要求メッセージに対応する鍵生成応答メッセージと、認証要求メッセージに対応する認証応答メッセージと、鍵要求メッセージに対応する鍵応答メッセージとを含み、鍵交換代行処理手段は、開始要求メッセージに基づいて、暗号通信における鍵交換方法を決定する鍵交換方法決定手段と、鍵生成要求メッセージに基づいて、共通鍵を生成する共通鍵生成手段と、認証要求メッセージに基づいて、第１の情報処理装置の通信相手である他の情報処理装置を認証する認証手段と、認証要求メッセージに基づいて、第１の情報処理装置の通信相手である他の情報処理装置が第１の情報処理装置にアクセス可能か否かを確認する確認手段と、鍵要求メッセージに基づいて、セッション鍵に関する処理を行うセッション鍵処理手段とを備えるようにすることができる。

【００２４】前記鍵交換方法は、IKE、または、SSL若しくはTLSのHandshake Protocolを含むようにすることができる。

【００２５】前記第１の情報処理装置は、第２の情報処理装置と安全に通信が行えるか否かを判定する第１の判定手段と、第１の判定手段の判定結果に基づいて、第２の情報処理装置と安全に通信するための、第２の情報処理装置と共有する共通鍵を設定する第１の共通鍵設定手段とをさらに備え、第２の情報処理装置は、第１の情報処理装置と安全に通信が行えるか否かを判定する第２の判定手段と、第２の判定手段の判定結果に基づいて、第１の情報処理装置と安全に通信するための、第１の情報処理装置と共有する共通鍵を設定する第２の共通鍵設定

手段とをさらに備えるようにすることができる。

【００２６】本発明の第１の情報処理装置は、第１の他の情報処理装置と暗号通信を行う暗号通信手段と、暗号通信手段による暗号通信に用いる共通鍵を記憶する記憶手段と、共通鍵を第１の他の情報処理装置と共有するための鍵交換処理の代行を要求する要求メッセージを、鍵交換処理を代行する第２の他の情報処理装置に供給する要求メッセージ供給手段と、要求メッセージ供給手段により供給された要求メッセージに対応する応答メッセージを、第２の他の情報処理装置より取得する応答メッセージ取得手段と、応答メッセージ取得手段により取得された応答メッセージに基づいて、暗号通信のセッションごとの共通鍵であるセッション鍵を設定するセッション鍵設定手段とを備えることを特徴とする。

【００２７】前記第１の情報処理装置は、前記第２の他の情報処理装置と安全に通信が行えるか否かを判定する判定手段と、判定手段の判定結果に基づいて、第２の他の情報処理装置と安全に通信するための、第２の他の情報処理装置と共有する共通鍵を設定する共通鍵設定手段とをさらに備えるようにすることができる。

【００２８】本発明の第１の情報処理方法は、第１の他の情報処理装置と暗号通信を行う暗号通信ステップと、暗号通信ステップの処理による暗号通信に用いる共通鍵の記憶部からの取得を制御する記憶制御ステップと、暗号通信ステップの処理による暗号通信に用いる共通鍵を第１の他の情報処理装置と共有するための鍵交換処理の代行を要求する要求メッセージを、鍵交換処理を代行する第２の他の情報処理装置に供給する要求メッセージ供給ステップと、要求メッセージ供給ステップの処理により供給された要求メッセージに対応する応答メッセージの、第２の他の情報処理装置からの取得を制御する応答メッセージ取得制御ステップと、応答メッセージ取得制御ステップの処理により取得が制御された応答メッセージに基づいて、暗号通信のセッションごとの共通鍵であるセッション鍵を設定するセッション鍵設定ステップとを含むことを特徴とする。

【００２９】本発明の第１の記録媒体のプログラムは、第１の他の情報処理装置と暗号通信を行う暗号通信ステップと、暗号通信ステップの処理による暗号通信に用いる共通鍵の記憶部からの取得を制御する記憶制御ステップと、暗号通信ステップの処理による暗号通信に用いる共通鍵を第１の他の情報処理装置と共有するための鍵交換処理の代行を要求する要求メッセージを、鍵交換処理を代行する第２の他の情報処理装置に供給する要求メッセージ供給ステップと、要求メッセージ供給ステップの処理により供給された要求メッセージに対応する応答メッセージの、第２の他の情報処理装置からの取得を制御する応答メッセージ取得制御ステップと、応答メッセージ取得制御ステップの処理により取得が制御された応答メッセージに基づいて、暗号通信のセッションごとの共通鍵であるセッション鍵を設定するセッション鍵設定ステップとを含むことを特徴とする。

【００３０】本発明の第１のプログラムは、第１の他の情報処理装置と暗号通信を行う暗号通信ステップと、暗号通信ステップの処理による暗号通信に用いる共通鍵の記憶部からの取得を制御する記憶制御ステップと、暗号通信ステップの処理による暗号通信に用いる共通鍵を第１の他の情報処理装置と共有するための鍵交換処理の代行を要求する要求メッセージを、鍵交換処理を代行する第２の他の情報処理装置に供給する要求メッセージ供給ステップと、要求メッセージ供給ステップの処理により供給された要求メッセージに対応する応答メッセージの、第２の他の情報処理装置からの取得を制御する応答メッセージ取得制御ステップと、応答メッセージ取得制御ステップの処理により取得が制御された応答メッセージに基づいて、暗号通信のセッションごとの共通鍵であるセッション鍵を設定するセッション鍵設定ステップとをコンピュータに実現させる。

【００３１】本発明の第２の情報処理装置は、鍵交換処理に関する情報を記憶する記憶手段と、鍵交換処理の代行を要求する要求メッセージを、第１の他の情報処理装置より取得する要求メッセージ取得手段と、要求メッセージ取得手段により取得された要求メッセージに基づいて、鍵交換処理を代行して行う鍵交換代行処理手段と、鍵交換代行処理手段の処理結果に基づいて、要求メッセージに対応する応答メッセージを、第１の他の情報処理装置に供給する応答メッセージ供給手段とを備えることを特徴とする。

【００３２】前記要求メッセージは、鍵交換処理の開始を示し、鍵交換方法の決定を要求する開始要求メッセージと、共通鍵の生成を要求する鍵生成要求メッセージと、第２の他の情報処理装置の認証を要求する認証要求メッセージと、暗号通信のセッションごとの共通鍵であるセッション鍵を要求する鍵要求メッセージとを含み、応答メッセージは、開始要求メッセージに対応する開始応答メッセージと、鍵生成要求メッセージに対応する鍵生成応答メッセージと、認証要求メッセージに対応する認証応答メッセージと、鍵要求メッセージに対応する鍵応答メッセージとを含み、鍵交換代行処理手段は、開始要求メッセージに基づいて、暗号通信における鍵交換方法を決定する鍵交換方法決定手段と、鍵生成要求メッセージに基づいて、共通鍵を生成する共通鍵生成手段と、認証要求メッセージに基づいて、第２の他の情報処理装置を認証する認証手段と、認証要求メッセージに基づいて、第２の他の情報処理装置が第１の他の情報処理装置にアクセス可能か否かを確認する確認手段と、鍵要求メッセージに基づいて、セッション鍵に関する処理を行うセッション鍵処理手段とを備えるようにすることができる。

【００３３】前記第２の情報処理装置は、第１の他の情

報処理装置と安全に通信が行えるか否かを判定する判定手段と、判定手段の判定結果に基づいて、第１の他の情報処理装置と安全に通信するための、第１の他の情報処理装置と共有する共通鍵を設定する共通鍵設定手段とをさらに備えるようにすることができる。

【００３４】前記記憶手段により記憶されている鍵交換処理に関する情報は、第２の他の情報処理装置の認証に関する情報、および第２の他の情報処理装置が第１の他の情報処理装置にアクセス可能か否かに関する情報であるポリシ情報を含むようにすることができる。

【００３５】本発明の第２の情報処理方法は、鍵交換処理に関する情報の記憶部からの取得を制御する記憶制御ステップと、鍵交換処理の代行を要求する要求メッセージの、第１の他の情報処理装置からの取得を制御する要求メッセージ取得制御ステップと、要求メッセージ取得制御ステップの処理により取得が制御された要求メッセージに基づいて、鍵交換処理を代行して行う鍵交換代行処理ステップと、鍵交換代行処理ステップの処理の処理結果に基づいて、要求メッセージに対応する応答メッセージを、第１の他の情報処理装置に供給する応答メッセージ供給ステップとを含むことを特徴とする。

【００３６】本発明の第２の記録媒体のプログラムは、鍵交換処理に関する情報の記憶部からの取得を制御する記憶制御ステップと、鍵交換処理の代行を要求する要求メッセージの、第１の他の情報処理装置からの取得を制御する要求メッセージ取得制御ステップと、要求メッセージ取得制御ステップの処理により取得が制御された要求メッセージに基づいて、鍵交換処理を代行して行う鍵交換代行処理ステップと、鍵交換代行処理ステップの処理の処理結果に基づいて、要求メッセージに対応する応答メッセージを、第１の他の情報処理装置に供給する応答メッセージ供給ステップとを含むことを特徴とする。

【００３７】本発明の第２のプログラムは、鍵交換処理に関する情報の記憶部からの取得を制御する記憶制御ステップと、鍵交換処理の代行を要求する要求メッセージの、第１の他の情報処理装置からの取得を制御する要求メッセージ取得制御ステップと、要求メッセージ取得制御ステップの処理により取得が制御された要求メッセージに基づいて、鍵交換処理を代行して行う鍵交換代行処理ステップと、鍵交換代行処理ステップの処理の処理結果に基づいて、要求メッセージに対応する応答メッセージを、第１の他の情報処理装置に供給する応答メッセージ供給ステップとをコンピュータに実現させる。

【００３８】本発明のネットワークシステムにおいては、ネットワークに接続され、他の情報処理装置と暗号通信を行う第１の情報処理装置と、ネットワークに接続され、第１の情報処理装置が暗号通信に用いる共通鍵を、通信相手である他の情報処理装置と共有するための、第１の情報処理装置による鍵交換処理を代行する第２の情報処理装置とが備えられ、第１の情報処理装置に

おいては、他の情報処理装置と暗号通信が行われ、鍵交換処理の代行を要求する要求メッセージが第２の情報処理装置に供給され、要求メッセージに対応する応答メッセージが、第２の情報処理装置より取得され、応答メッセージに基づいて、暗号通信に用いるセッションごとの共通鍵であるセッション鍵が設定され、第２の情報処理装置においては、要求メッセージが第１の情報処理装置より取得され、その要求メッセージに基づいて、鍵交換処理が代行して行われ、鍵交換代行処理手段の処理結果に基づいて、要求メッセージに対応する応答メッセージが、第１の情報処理装置に供給される。

【００３９】本発明の第１の情報処理装置および方法、並びにプログラムにおいては、第１の他の情報処理装置と暗号通信が行われ、暗号通信に用いる共通鍵が記憶され、共通鍵を第１の他の情報処理装置と共有するための鍵交換処理の代行を要求する要求メッセージが、鍵交換処理を代行する第２の他の情報処理装置に供給され、その要求メッセージに対応する応答メッセージが、第２の他の情報処理装置より取得され、その応答メッセージに基づいて、暗号通信のセッションごとの共通鍵であるセッション鍵が設定される。

【００４０】本発明の第２の情報処理装置および方法、並びにプログラムにおいては、鍵交換処理に関する情報が記憶され、鍵交換処理の代行を要求する要求メッセージが、第１の他の情報処理装置より取得され、その要求メッセージに基づいて、鍵交換処理が代行して行われる、鍵交換代行処理手段の処理結果に基づいて、要求メッセージに対応する応答メッセージが、第１の他の情報処理装置に供給される。

【００４１】

【発明の実施の形態】図１は、本発明を適用した鍵交換処理代行システムの構成例を表している。

【００４２】図１において、端末装置１は、インターネット等に代表されるネットワーク２に接続されており、ネットワーク２を介して、IPsec，SSL，またはTLS等により、通信相手側端末装置４と通信内容が暗号化された暗号通信を行う。鍵交換代行サーバ３は、ネットワーク２に接続されており、端末装置１が通信相手端末装置４と共通鍵を共有するために行う鍵交換処理の鍵生成処理や認証処理等を代行する。

【００４３】なお、図１において、ネットワーク２には、端末装置１、鍵交換代行サーバ３、および通信相手側端末装置４が1台ずつ接続されているが、これに限らず、端末装置１、鍵交換代行サーバ３、および通信相手側端末装置４がそれぞれ複数接続されていてもよい。

【００４４】図２は、端末装置１の構成例を示すブロック図である。

【００４５】図２において、CPU（Central Processing Unit）１１は、ROM（Read Only Memory）１２に記憶されているプログラム、または記憶部２３からRAM（Rando

m Access Memory）１３にロードされたプログラムに従って各種の処理を実行する。RAM１３にはまた、CPU１１が各種の処理を実行する上において必要なデータなども適宜記憶される。CPU１１、ROM１２、およびRAM１３は、バス１４を介して相互に接続されている。このバス１４にはまた、入出力インタフェース２０も接続されている。

【００４６】入出力インタフェース２０には、キーボード、マウスなどよりなる入力部２１、CRT（Cathode Ray Tube）、LCD（Liquid Crystal Display）などよりなるディスプレイ、並びにスピーカなどよりなる出力部２２、ハードディスクなどより構成される記憶部２３、モデム、ターミナルアダプタなどより構成される通信部２４、および、メモリやハードディスク等で構成される暗号鍵データベース２５が接続されている。通信部２４は、ネットワーク２を介しての通信処理を行う。通信部２４はまた、他のユーザ端末との間で、アナログ信号またはデジタル信号の通信処理を行う。また、暗号鍵データベース２５は、鍵交換代行サーバ３、または通信相手側端末装置４との通信の内容を暗号化するための鍵情報を記録している。

【００４７】入出力インタフェース２０にはまた、必要に応じてドライブ３０が接続され、磁気ディスク４１、光ディスク４２、光磁気ディスク４３、或いは半導体メモリ４４などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部２３にインストールされる。

【００４８】図３は、鍵交換代行サーバ３の構成例を示すブロック図である。

【００４９】図３において、鍵交換代行サーバ３は、図２の端末装置１のCPU１１乃至通信部２４に対応するCPU５１乃至通信部６４を有しており、その基本的構成は、端末装置１と同様であるので、その説明は省略する。

【００５０】また、図３において、入出力インタフェース６０は、さらに、データベース６５を有している。データベース６５は、端末装置１との通信の内容を暗号化するための鍵情報に関する情報、通信相手側端末装置４を認証する認証鍵に関する情報、および、端末装置１へのアクセスが許可された装置に関する情報等が記憶されている。

【００５１】さらに、入出力インタフェース６０には、必要に応じてドライブ７０が接続され、磁気ディスク８１、光ディスク８２、光磁気ディスク８３、或いは半導体メモリ８４などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部６３にインストールされる。

【００５２】なお、図示は省略するが、通信相手側端末装置４も、図２に示した端末装置１と基本的に同様の構成を有するコンピュータにより構成される。

【００５３】次に、図４および図５のフローチャートを

参照して、端末装置１による鍵交換代行処理を説明する。また、必要に応じて、図６および図７を参照して説明する。

【００５４】通信相手側端末装置４と鍵交換を行う端末装置１のCPU１１は、最初に、ステップＳ１において、鍵交換代行サーバ３との間に安全な通信路が確保されるか否かを判定する。

【００５５】確保されないと判定した場合、CPU１１は、ステップＳ２に進み、鍵交換代行サーバ３と安全に通信するための鍵を暗号鍵データベース２５に設定し、ステップＳ３に進む。なお、設定される鍵は、予め決められており、鍵交換代行サーバ３と暗号通信ができるように、鍵交換代行サーバ３に設定される鍵と対応してある。また、ステップＳ１において、鍵交換代行サーバ３との間に安全な通信路が確保されると判定した場合、CPU１１は、ステップＳ３に進む。

【００５６】すなわち、端末装置１と鍵交換代行サーバ３との間が安全な通信路である場合、両者間の通信は、通常の通信により行われるが、端末装置１と鍵交換代行サーバ３との間が安全な通信路でない場合は、通信内容を暗号化した暗号通信により行われる。

【００５７】図６は、端末装置１と鍵交換代行サーバ３との間が安全な通信路である場合の端末装置１の通信に関する主な処理の流れを示す図である。

【００５８】図６において、安全な通信路を用いて鍵交換代行サーバ３に情報を供給する場合、CPU１１の処理部１０１は、通信部２４を介して、鍵交換代行サーバ３に情報を供給する。また、安全な通信路を用いて鍵交換代行サーバ３より情報を取得する場合、CPU１１の処理部１０１は、通信部２４を介して、鍵交換代行サーバ３より情報を取得する。

【００５９】通信相手側端末装置４に情報を供給する場合、CPU１１の処理部１０１は、暗号通信部１０２に情報を供給する。暗号通信部１０２は、暗号鍵データベース２５より必要な鍵情報を取得し、処理部１０１より供給された情報を暗号化する。情報を暗号化した暗号通信部１０２は、通信部２４を介して、暗号化した情報を通信相手側端末装置４に供給する。また、通信相手側端末装置４より情報を取得する場合、供給された情報は、通信部２４を介して暗号通信部１０２に供給される。暗号通信部１０２は、暗号鍵データベース２５より必要な鍵情報を取得し、通信部２４を介して供給された情報を復号し、処理部１０１に供給する。

【００６０】すなわち、端末装置１は、通信相手側端末装置４と暗号通信を行い、鍵交換代行サーバ３と暗号化されていない通常の通信を行う。

【００６１】また、図７は、端末装置１と鍵交換代行サーバ３との間が安全な通信路でない場合の端末装置１の通信に関する主な処理の流れを示す図である。

【００６２】図７において、鍵交換代行サーバ３または

通信相手側端末装置４に情報を供給する場合、CPU１１の処理部１０１は、暗号通信部１０２に情報を供給し、暗号鍵データベース２５より必要な鍵情報を取得させ、供給した情報を暗号化させる。そして、情報を暗号化した暗号通信部１０２は、通信部２４を介して、暗号化した情報を鍵交換代行サーバ３または通信相手側端末装置４に供給する。また、鍵交換代行サーバ３または通信相手側端末装置４より情報を取得する場合、供給された情報は、通信部２４を介して暗号通信部１０２に供給される。暗号通信部１０２は、暗号鍵データベース２５より必要な鍵情報を取得し、通信部２４を介して供給された情報を復号し、処理部１０１に供給する。

【００６３】すなわち、端末装置１は、鍵交換代行サーバ３および通信相手側端末装置４のいずれの場合も暗号通信を行う。従って、この場合、ステップＳ３以降の処理において、端末装置１と鍵交換代行サーバ３の間の通信は、全て暗号化されて行われる。以下の説明において、端末装置１が行う暗号化および復号する処理は図７において説明した場合と同様であるので、その説明は省略する。

【００６４】図４に戻り、ステップＳ３において、CPU１１は、鍵交換代行サーバ３に鍵交換処理の開始を示し、鍵交換方法の決定を要求する開始要求メッセージを供給する。開始要求メッセージには、端末装置１において利用可能な暗号化アルゴリズムやハッシュアルゴリズムのリスト等が含まれている。

【００６５】開始要求メッセージを供給したCPU１１は、ステップＳ４において、通信部２４を制御して、開始要求メッセージに対応する応答メッセージである開始応答メッセージを取得したか否かを判定し、取得したと判定するまで待機する。

【００６６】開始応答メッセージには、鍵交換方法に関する情報や、使用するアルゴリズムの情報等が含まれており、CPU１１は、この開始応答メッセージに基づいて各種の処理を行う。

【００６７】通信部２４を制御して、開始応答メッセージを取得したと判定した場合、CPU１１は、ステップＳ５に進み、取得した開始応答メッセージに含まれる鍵交換方法に基づいて、鍵生成処理が必要か否かを判定する。鍵生成処理は、通信相手側端末装置４と共有する共通鍵を生成する処理である。必要な場合、CPU１１は、ステップＳ６に進み、通信部２４を制御して、鍵交換代行サーバ３に鍵生成処理の代行を要求する鍵生成要求メッセージを供給する。鍵生成要求メッセージを供給したCPU１１は、ステップＳ７において、通信部２４を制御して、鍵生成要求メッセージに対応する鍵生成応答メッセージを取得したか否かを判定し、取得するまで待機する。取得したと判定した場合、CPU１１は、図５のステップＳ１２に進む。

【００６８】また、図４のステップＳ５において、鍵生成処理が必要ないと判定した場合、CPU１１は、図５のステップＳ８に進み、開始応答メッセージに含まれる鍵交換方法に基づいて、認証処理が必要か否かを判定する。必要と判定した場合、CPU１１は、ステップＳ９に進み、通信部２４を制御して、鍵交換代行サーバ３に、通信相手側端末装置４を認証する認証処理の代行を要求する認証要求メッセージを供給する。

【００６９】認証処理の代行を要求したCPU１１は、ステップＳ１０に進み、通信部２４を制御して、認証要求メッセージに対応する認証応答メッセージを取得したか否かを判定し、取得したと判定するまで待機する。そして、取得したと判定した場合、CPU１１は、ステップＳ１１に進み、認証応答メッセージを参照して、通信相手側端末装置４が認証されたか否かを判定する。認証されたと判定した場合、CPU１１は、ステップＳ１２に進む。

【００７０】ステップＳ１２において、CPU１１は、以上の処理により、鍵交換処理において必要な情報が全て揃ったか否かを判定し、揃っていないと判定した場合、図４のステップＳ５に戻り、それ以降の処理を繰り返す。

【００７１】全ての情報が揃ったと判定した場合、CPU１１は、ステップＳ１３に進み、通信部２４を制御して、鍵交換代行サーバ３に、通信相手側端末装置４との暗号通信において使用されるセッションごとの鍵であるセッション鍵を要求する鍵要求メッセージを供給する。鍵要求メッセージを供給したCPU１１は、ステップＳ１４において、通信部２４を制御して、鍵要求メッセージに対応する鍵応答メッセージを取得したか否かを判定し、取得したと判定するまで待機する。

【００７２】取得したと判定した場合、CPU１１は、ステップＳ１５に進み、開始応答メッセージに含まれる鍵交換方法において、鍵応答メッセージの内容に基づいてセッション鍵を生成する必要があるか否かを判定する。生成する必要があると判定した場合、CPU１１は、ステップＳ１６に進み、鍵応答メッセージに基づいて、セッション鍵を生成し、ステップＳ１７に進む。また、ステップＳ１５において、鍵応答メッセージにセッション鍵が含まれており、セッション鍵を生成する必要がないと判定した場合、CPU１１は、ステップＳ１７に進む。

【００７３】ステップＳ１７において、CPU１１は、通信相手側端末装置４と安全に通信するためのセッション鍵を暗号鍵データベース２５に設定し、鍵交換代行処理を終了する。

【００７４】また、図５のステップＳ８において、開始応答メッセージに含まれる鍵交換方法に基づいて、認証処理が必要でないと判定した場合、本来ありえない状態であるので、CPU１１は、ステップＳ１８において、誤動作しているとして扱う誤動作処理を行い、ステップＳ１９においてエラー処理を行い、鍵交換代行処理を終了

する。

【００７５】また、図５のステップＳ１１において、通信相手側端末装置４が認証されなかったと判定した場合、CPU１１は、ステップＳ１９に進み、エラー処理を行い、鍵交換代行処理を終了する。

【００７６】次に、図８および図９のフローチャートを参照して、上述した端末装置による鍵交換代行処理に対応する鍵交換代行サーバ３による鍵交換代行処理について説明する。また、必要に応じて、図１０および図１１を参照して説明する。

【００７７】端末装置１の鍵交換処理を代行するCPU５１は、最初に、ステップＳ３１において、端末装置１との間に安全な通信路が確保されるか否かを判定する。

【００７８】確保されないと判定した場合、CPU５１は、ステップＳ３２に進み、端末装置１と安全に通信するための鍵をデータベース６５に設定し、ステップＳ３３に進む。なお、設定される鍵は、予め決められており、端末装置１と暗号通信ができるように、端末装置１に設定される鍵と対応してある。また、ステップＳ３１において、端末装置１との間に安全な通信路が確保されると判定した場合、CPU５１は、ステップＳ３３に進む。

【００７９】上述したように、端末装置１と鍵交換代行サーバ３との間が安全な通信路でない場合は、通信内容を暗号化した暗号通信により行われる。

【００８０】図１０は、端末装置１と鍵交換代行サーバ３との間が安全な通信路である場合の鍵交換代行サーバ３の通信に関する主な処理の流れを示す図である。

【００８１】図１０において、CPU５１には、各種の処理を実行する処理部１２１、鍵を生成する鍵生成部１２２、および認証処理を行う認証部１２３が構成されている。また、データベース６５には、認証部１２３による認証処理に用いられる認証鍵を管理する認証鍵データベース１３１、および端末装置１にアクセスすることを許可された装置に関する情報が管理されているポリシーデータベース１３２が設けられている。

【００８２】安全な通信路を用いて端末装置１に情報を供給する場合、CPU５１の処理部１２１は、通信部６４を介して、端末装置１に情報を供給する。例えば、処理部１２１は、鍵生成部１２２において生成された鍵を含むメッセージを、通信部６４を介して、端末装置１に供給する。また、安全な通信路を用いて端末装置１より情報を取得する場合、CPU５１の処理部１２１は、通信部２４を介して、端末装置１より情報を取得する。

【００８３】例えば、処理部１２１は、通信部６４を介して端末装置１より取得した証明書等を認証部１２３に供給する。認証部１２３は、データベース６５の認証鍵データベース１３１に登録されている認証鍵に基づいて、通信相手側端末装置４の認証を行い、その認証結果を処理部１２１に供給する。また、処理部１２１は、データベース１３２のポリシデータベース１３２に登録されている端末装置１のポリシに関する情報に基づいて、通信相手側端末装置４が端末装置１にアクセス可能か否かを判定する。

【００８４】すなわち、鍵交換代行サーバ３は、端末装置１と暗号化されていない通常の通信を行う。

【００８５】また、図１１は、端末装置１と鍵交換代行サーバ３との間が安全な通信路でない場合の鍵交換代行サーバ３の通信に関する主な処理の流れを示す図である。

【００８６】図１１において、CPU５１には、処理部１２１、鍵生成部１２２、および認証部１２３の他に、処理部１２１と通信部６４の間に、情報を暗号化する暗号通信部１４１が構成されている。また、データベース６５には、認証鍵データベース１３１、ポリシデータベース１３２、および、暗号鍵を管理する暗号鍵データベース１４２が設けられている。暗号通信部１４１は、暗号鍵データベース１４２に設定されている暗号鍵に基づいて、情報の暗号化を行う。

【００８７】すなわち、鍵交換代行サーバ３は、端末装置１との通信において、暗号通信を行う。従って、この場合、ステップＳ３３以降の処理において、端末装置１と鍵交換代行サーバ３の間の通信は、全て暗号化されて行われる。以下の説明において、鍵交換代行サーバ３による暗号化および復号する処理は図１１において説明した場合と同様であるので、その説明は省略する。

【００８８】図８に戻り、ステップＳ３３において、CPU５１は、通信部６４を制御して、端末装置１よりメッセージを取得したか否かを判定し、取得したと判定するまで待機する。取得したと判定した場合、CPU５１は、ステップＳ３４に進み、取得したメッセージが開始要求メッセージか否かを判定する。取得したメッセージが、図４のステップＳ３において、端末装置１より供給された開始要求メッセージであると判定した場合、CPU５１は、ステップＳ３５に進み、ステップＳ３５において、取得した開始要求メッセージに基づいて、通信相手側端末装置４との鍵交換方法を決定し、それを含む開始応答メッセージを生成する。そして、ステップＳ３６に進み、CPU５１は、通信部６４を制御して、生成した開始応答メッセージを端末装置１に供給する。

【００８９】そして、ステップＳ３７において、CPU５１は、鍵交換代行処理を終了するか否かを判定し、終了しない場合は、ステップＳ３３に戻り、それ以降の処理を繰り返す。また、ステップＳ３７において、終了すると判定した場合、CPU５１は、鍵交換代行処理を終了する。

【００９０】図８のステップＳ３４において、取得したメッセージは開始要求メッセージではないと判定した場合、CPU５１は、ステップＳ３８に進む。ステップＳ３８において、CPU５１は、取得したメッセージが鍵生成

要求メッセージか否かを判定する。鍵生成要求メッセージであると判定した場合、CPU５１は、ステップＳ３９に進み、鍵生成要求メッセージに基づいて、鍵を生成する。そして、ステップＳ４０において、CPU５１は、生成した鍵を含む鍵生成応答メッセージを、通信部６４を介して端末装置１に供給する。端末装置１に鍵生成応答メッセージを供給したCPU５１は、ステップＳ３７に戻り、それ以降の処理を繰り返す。

【００９１】また、図８のステップＳ３８において、取得したメッセージは鍵生成要求メッセージではないと判定した場合、CPU５１は、図９のステップＳ４１に進む。図９のステップＳ４１において、CPU５１は、取得したメッセージが認証要求メッセージであるか否かを判定する。認証要求メッセージであると判定した場合、CPU５１は、ステップＳ４２に進み、図１０のデータベース６５の認証鍵データベース１３１に保持されている認証鍵を利用して認証処理を行う。そして、ステップＳ４３において、CPU５１は、ポリシデータベース４３により保持されているポリシを確認し、通信相手側端末装置による端末装置へのアクセスが許可されているか否かを確認する処理を行い、ステップＳ４４において、認証結果および確認結果を含む認証応答メッセージを、通信部６４を制御して、端末装置１に供給する。端末装置１に認証応答メッセージを供給したCPU５１は、ステップＳ３７に戻り、それ以降の処理を繰り返す。

【００９２】ステップＳ４１において、取得したメッセージが認証要求メッセージではないと判定した場合、CPU５１は、ステップＳ４５に進み、取得したメッセージが鍵要求メッセージか否かを判定する。鍵要求メッセージであると判定した場合、CPU５１は、ステップＳ４６に進み、図８のステップＳ３５において決定した鍵交換方法に基づいて、セッション鍵を生成する必要があるか否かを判定する。そして、必要があると判定した場合、CPU５１は、ステップＳ４７に進み、通信相手側端末装置４との通信に利用するセッション鍵を生成し、ステップＳ４８に進む。また、生成する必要がないと判定した場合、CPU５１は、ステップＳ４８に進む。そして、ステップＳ４８において、CPU５１は、上述した処理の結果を踏まえた鍵応答メッセージを生成し、通信部６４を制御して、端末装置に供給する。鍵応答メッセージを端末装置１に供給したCPU５１は、ステップＳ３７に戻り、それ以降の処理を繰り返す。

【００９３】また、ステップＳ４５において、取得したメッセージが鍵要求メッセージではないと判定した場合、CPU５１は、ステップＳ４９において、この不明なメッセージを破棄し、ステップＳ３７に戻り、それ以降の処理を繰り返す。

【００９４】以上のように、端末装置１および鍵交換代行サーバ３において鍵交換代行処理を行うことにより、鍵交換処理における端末装置１の負担を軽減することができる。

【００９５】次に、図１２乃至図１４を参照して、上述した鍵交換処理代行システムの既存の鍵交換処理への適用例を説明する。

【００９６】図１２は、本発明を適用した鍵交換処理代行システムのIKEへの適用例を示す図である。図１２においては、端末装置１が通信相手側端末装置４とIKEにより鍵交換を行う際に、鍵交換代行サーバ３により、端末装置１が行うPhase１の鍵交換処理の一部を代行している。

【００９７】最初に、ステップＳ１０１において、通信相手側端末装置４が通信を保護するために用いられる方針や鍵の集合からなる情報を含むSAペイロードを端末装置１に供給し、端末装置１は、ステップＳ１２１において、そのSAペイロードを取得する。

【００９８】SAペイロードを受信すると端末装置１は、ステップＳ１２２で、SAペイロードや利用可能な暗号化アルゴリズム等を含む開始要求メッセージを鍵交換代行サーバ３に供給する。この処理は、図４のステップＳ３の処理に対応する。鍵交換代行サーバ３は、ステップＳ１５１において、端末装置１より供給された開始要求メッセージを取得すると、決定した鍵交換方法等の情報を含む返信用のSAペイロードを生成し、その返信用SAペイロードを含む開始応答メッセージを生成して端末装置１に供給する。この処理は、図８のステップＳ３４乃至ステップＳ３６の処理に対応する。

【００９９】鍵交換代行サーバ３より供給された開始応答メッセージは、端末装置１によりステップＳ１２３において取得される。この処理は、図４のステップＳ４の処理に対応する。そして、開始応答メッセージを取得した端末装置１は、ステップＳ１２４において、開始応答メッセージに含まれる返信用のSAペイロードを通信相手側端末装置４にIKEのSAペイロードとして供給する。

【０１００】通信相手側端末装置４は、ステップＳ１０２において、そのSAペイロードを取得すると、ステップＳ１０３において、共有秘密として使用される鍵情報を含む鍵交換ペイロード、および、乱数情報を含むNonceペイロードを端末装置１に供給する。端末装置１は、ステップＳ１２５において、その鍵交換ペイロードおよびNonceペイロードを取得する。端末装置１は、ステップＳ１２６において、取得した鍵交換ペイロードを含む鍵生成要求メッセージを鍵交換代行サーバ３に供給する。この処理は、図４のステップＳ６の処理に対応する。鍵交換代行サーバ３は、ステップＳ１５３において、端末装置１より供給された鍵生成要求メッセージを取得すると、返信用の鍵交換ペイロードを生成し、ステップＳ１５４において、作成した返信用の鍵交換ペイロードを含む鍵生成応答メッセージを端末装置１に供給する。また、鍵交換ペイロードの内容に基づいて、ISAKMP SAを生成する。これらの処理は、図８のステップＳ３８乃至

ステップＳ４０の処理に対応する。

【０１０１】端末装置１は、ステップＳ１２７において鍵生成応答メッセージを取得する。この処理は図４のステップＳ７の処理に対応する。端末装置１は、ステップＳ１２８において、鍵生成応答メッセージに含まれる返信用の鍵交換ペイロードおよびNonceペイロードを通信相手側端末装置４に供給する。通信相手側端末装置４は、この返信用の鍵交換ペイロードおよびNonceペイロードをステップＳ１０４において取得すると、ステップＳ１０５において、IDペイロードおよび署名ペイロードを端末装置１に供給する。

【０１０２】端末装置１は、ステップＳ１２９において、IDペイロードおよび署名ペイロードを取得すると、ステップＳ１３０において、署名ペイロードを含む認証要求メッセージを鍵交換代行サーバ３に供給する。この処理は、図５のステップＳ９の処理に対応する。ステップＳ１５５において、鍵交換代行サーバ３は、端末装置１より供給された認証要求メッセージを取得すると、認証要求メッセージに含まれる署名に基づいて認証処理を行い、認証されると返信用の署名ペイロードを生成し、ステップＳ１５６において、生成した返信用の署名ペイロードを含む認証応答メッセージを端末装置１に供給する。この処理は、図９のステップＳ４１乃至ステップＳ４４の処理に対応する。

【０１０３】ステップＳ１３１において、端末装置１は、鍵交換代行サーバ３より供給された認証応答メッセージを取得する。この処理は、図５のステップＳ１０の処理に対応する。端末装置１は、ステップＳ１３２においてIDペイロードおよび署名ペイロードを通信相手側端末装置４に供給する。通信相手側端末装置４は、そのIDペイロードおよび署名ペイロードを、ステップＳ１０６において、取得する。

【０１０４】また、端末装置１は、ステップＳ１３３において、鍵交換代行サーバ３に鍵要求メッセージを供給する。この処理は、図５のステップＳ１３の処理に対応する。鍵交換代行サーバ３は、ステップＳ１５７において、端末装置１より鍵要求メッセージを取得すると、セッション鍵を生成し、ステップＳ１５８において、端末装置１に鍵応答メッセージを供給する。この処理は、図９のステップＳ４５乃至ステップＳ４８の処理に対応する。そして、端末装置１は、鍵交換代行サーバ３より供給された鍵応答メッセージをステップＳ１３４において取得する。この処理は、図５のステップＳ１４の処理に対応する。

【０１０５】端末装置１は、鍵応答メッセージに含まれるISAKMP SAを設定し、Phase2の通信に利用する。

【０１０６】図１３は、図１２に示した処理に続いて行われるPhase2の処理の例を示す図である。Phase2においては、認証に関連する情報のみが交換される。

【０１０７】図１３において、通信相手側端末装置４は、ステップＳ１７１において、その状況下でトラフィックを保護するのに適していると考えるProposalを生成し、ハッシュペイロード、SAペイロード、およびNonceペイロードを端末装置１に供給する。端末装置１は、ステップＳ１９１において、これらのハッシュペイロード、SAペイロード、およびNonceペイロードを取得する。

【０１０８】そして、端末装置１は、ステップＳ１９２において、それが受け入れる保護スートを指示するために、返信用のハッシュペイロード、SAペイロード、およびNonceペイロードを通信相手側端末装置４に供給する。通信相手側端末装置４は、これらの返信用のハッシュペイロード、SAペイロード、およびNonceペイロードを、ステップＳ１７２において、取得する。

【０１０９】最後に、通信相手側端末装置４は、ステップＳ１７３において、ハッシュペイロードを端末装置１に供給し、端末装置１は、そのハッシュペイロードをステップＳ１９３において取得する。

【０１１０】以上のように、本発明を適用した鍵交換処理代行システムは、IKEによる鍵交換に適用される。

【０１１１】図１４は、本発明を適用した鍵交換処理代行システムのTLS Handshake Protocolへの適用例を示す図である。図１４においては、端末装置１が通信相手側端末装置４とTLS Handshake Protocolにより鍵交換を行う際に、鍵交換代行サーバ３により、端末装置１が行う鍵交換処理の一部を代行している。このとき、端末装置１がTLSクライアントとなり、通信相手側端末装置４がTLSサーバとなっている。

【０１１２】最初に、端末装置１は、ステップＳ３３１において、利用可能な暗号化アルゴリズム等を含めた開始要求メッセージを鍵交換代行サーバ３に供給する。この処理は、図４のステップＳ３の処理に対応する。鍵交換代行サーバ３は、ステップＳ３５１において、この開始要求メッセージを取得すると、開始要求メッセージに含まれている暗号化アルゴリズム等と、鍵交換代行サーバ３において利用可能な暗号化アルゴリズム等とから、TLS Handshake Protocolで利用するアルゴリズムを決定し、開始応答メッセージに含めて端末装置１に供給する。これらの処理は、図８のステップＳ３４乃至ステップＳ３６の処理に対応する。

【０１１３】端末装置１は、ステップＳ３２２において、鍵交換代行サーバ３より供給された開始応答メッセージを取得する。この処理は、図４のステップＳ４の処理に対応する。開始応答メッセージを取得した端末装置１は、ステップＳ３２３において、開始応答メッセージの内容に基づいて、TLS Handshake ProtocolのClientHelloメッセージを生成し、通信相手側端末装置４に供給する。通信相手側端末装置４は、このClientHelloメッセージをステップＳ３０１において取得すると、ステップＳ３０２において、ServerHelloメッセージを端末装

置１に供給し、Certificateメッセージを端末装置１に供給し、ServerHelloDoneメッセージを端末装置１に供給する。端末装置１は、それらのメッセージを、ステップＳ３２４において取得する。

【０１１４】Certificateメッセージを取得した端末装置１は、ステップＳ３２５において、取得したCertificateメッセージを含めた認証要求メッセージを鍵交換代行サーバ３に供給する。この処理は、図５のステップＳ９の処理に対応する。鍵交換代行サーバ３は、ステップＳ３５３において、この認証要求メッセージを取得し、認証要求メッセージに含まれるTLS Handshake ProtocolのCertificateメッセージに基づいて、通信相手側端末装置４を認証し、ステップＳ３５４において、認証結果を含めた認証応答メッセージを端末装置１に供給する。これらの処理は、図９のステップＳ４１乃至ステップＳ４４の処理に対応する。

【０１１５】ステップＳ３２６において、端末装置１は、認証応答メッセージを取得する。この処理は、図５のステップＳ１０の処理に対応する。端末装置１は、ステップＳ３２７において、pre-master keyを生成するために、鍵生成要求メッセージを鍵交換代行サーバ３に供給する。鍵交換代行サーバ３は、ステップＳ３５５において、鍵生成要求メッセージを取得すると、取得した鍵生成応答メッセージの内容に基づいて、TLS Handshake ProtocolのClient Key Exchangeメッセージに必要な情報を算出し、ステップＳ３５６において、その情報を含めた鍵生成応答メッセージを端末装置１に供給する。これらの処理は、図８のステップＳ３８乃至ステップＳ４０の処理に対応する。

【０１１６】鍵交換代行サーバ３より供給された鍵生成応答メッセージは、ステップＳ３２８において、端末装置１により取得される。この処理は、図４のステップＳ７の処理に対応する。端末装置１は、取得した鍵生成応答メッセージの内容に基づいて、TLS Handshake ProtocolのClient Key Exchangeメッセージを生成し、ステップＳ３２９において、生成したClient Key Exchangeメッセージを通信相手側端末装置４に供給する。通信相手側端末装置４は、このClient Key Exchangeメッセージを、ステップＳ３０３において取得する。

【０１１７】端末装置１は、ステップＳ３３０において、さらに、TLS Record Protocolで利用されるpre-master keyから生成される各種鍵情報を要求するための鍵要求メッセージを鍵交換代行サーバ３に送信する。この処理は、図５のステップＳ１３の処理に対応する。鍵交換代行サーバ３は、ステップＳ３５７において、この鍵要求メッセージを取得し、pre-master keyからTLS Record Protocolで利用するセッション鍵を生成し、ステップＳ３５８において、生成したセッション鍵を含む鍵応答メッセージを端末装置１に供給する。これらの処理は、図９のステップＳ４５乃至ステップＳ４８の処理に対応する。

【０１１８】端末装置１は、ステップＳ３３１において、鍵交換代行サーバ３に供給された鍵応答メッセージを取得し、取得した鍵応答メッセージの内容に基づいて、TLSRecord Protocolで利用するセッション鍵を設定する。これらの処理は、図５のステップＳ１５乃至ステップＳ１７の処理に対応する。

【０１１９】以上のように、本発明を適用した鍵交換処理代行システムは、TLS HandshakeProtocolによる鍵交換に適用される。

【０１２０】一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウエアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、ネットワークや記録媒体からインストールされる。

【０１２１】この記録媒体は、図２および図３に示すように、装置本体とは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク４１および８１（フロッピディスクを含む）、光ディスク４２および８２（CD-ROM(Compact Disc-Read Only Memory),DVD(Digital Versatile Disc)を含む）、光磁気ディスク４３および８３（ＭＤ（Mini-Disc）を含む）、もしくは半導体メモリ４４および８４などよりなるパッケージメディアにより構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに提供される、プログラムが記録されているCPU１１および５１に内蔵されているROMなどで構成される。

【０１２２】なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０１２３】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【０１２４】

【発明の効果】以上のように、本発明のネットワークシステムによれば、通信を行う情報処理装置の鍵交換処理による負担を軽減することができ、計算資源が限られた機器においても、既存の鍵交換プロトコルとの互換性を保ちつつ鍵交換を実現することができる。

【０１２５】本発明の第１の情報処理装置および方法、記録媒体、並びにプログラムによれば、鍵交換処理による負担を軽減することができ、計算資源が限られた機器である場合も、既存の鍵交換プロトコルとの互換性を保ちつつ鍵交換を実現することができる。

【０１２６】本発明の第２の情報処理装置および方法、記録媒体、並びにプログラムによれば、通信を行う情報

処理装置の鍵交換処理による負担を軽減することができ、計算資源が限られた機器においても、既存の鍵交換プロトコルとの互換性を保ちつつ鍵交換を実現することができる。

【図面の簡単な説明】

【図１】本発明を適用した鍵交換処理代行システムの構成例を表している。

【図２】図１の端末装置の構成例を示すブロック図である。

【図３】図１の鍵交換代行サーバの構成例を示すブロック図である。

【図４】端末装置による鍵交換代行処理を説明するフローチャートである。

【図５】端末装置による鍵交換代行処理を説明する、図４に続くフローチャートである。

【図６】端末装置と鍵交換代行サーバとの間が安全な通信路である場合の、端末装置の通信に関する主な処理の流れを示す図である。

【図７】端末装置と鍵交換代行サーバとの間が安全な通信路でない場合の、端末装置の通信に関する主な処理の流れを示す図である。

【図８】鍵交換代行サーバによる鍵交換代行処理について説明するフローチャートである。

【図９】鍵交換代行サーバによる鍵交換代行処理について説明する、図８に続くフローチャートである。

＊【図１０】端末装置と鍵交換代行サーバとの間が安全な通信路である場合の、鍵交換代行サーバの通信に関する主な処理の流れを示す図である。

【図１１】端末装置と鍵交換代行サーバとの間が安全な通信路でない場合の、鍵交換代行サーバの通信に関する主な処理の流れを示す図である。

【図１２】本発明を適用した鍵交換処理代行システムのIKEへの適用方法の例を説明するフローチャートである。

【図１３】図１２の処理に続く処理の例を説明するフローチャートである。

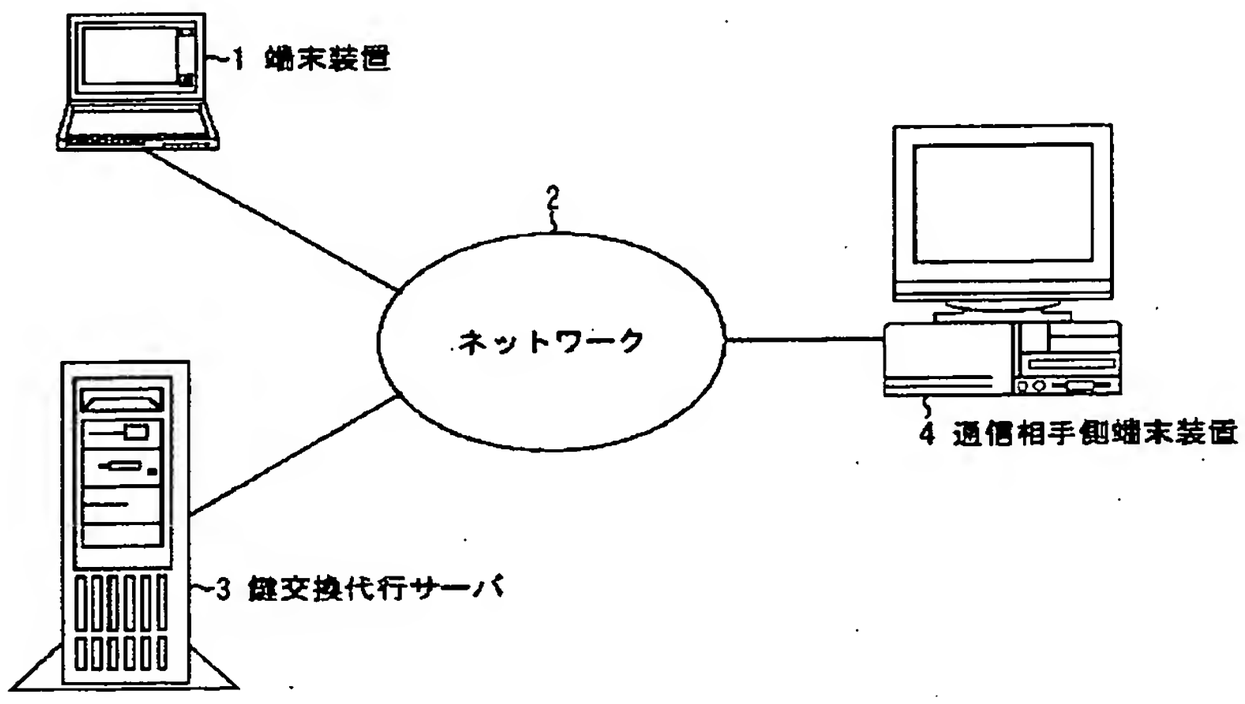
【図１４】本発明を適用した鍵交換処理代行システムのTLS Handshake Protocolへの適用方法の例を説明するフローチャートである。

【符号の説明】

１　端末装置，　２　ネットワーク，　３　鍵交換代行サーバ，　４　通信相手側端末装置，　１１　CPU，　１２　ROM，　１３　RAM，　２３　記憶部，２４　通信部，　２５　暗号鍵データベース，　５１　CPU，　５２　ROM，　５３　RAM，　６３　記憶部，　６４　通信部，　６５　データベース，　１０１処理部，　１０２　暗号通信部，　１２１　処理部，　１２２　鍵生成部，１２３　認証部，　１３１　認証鍵データベース，　１３２　ポリシデータベース，　１４１　暗号通信部，　１４２　暗号鍵データベース

【図１】

図一



【図２】

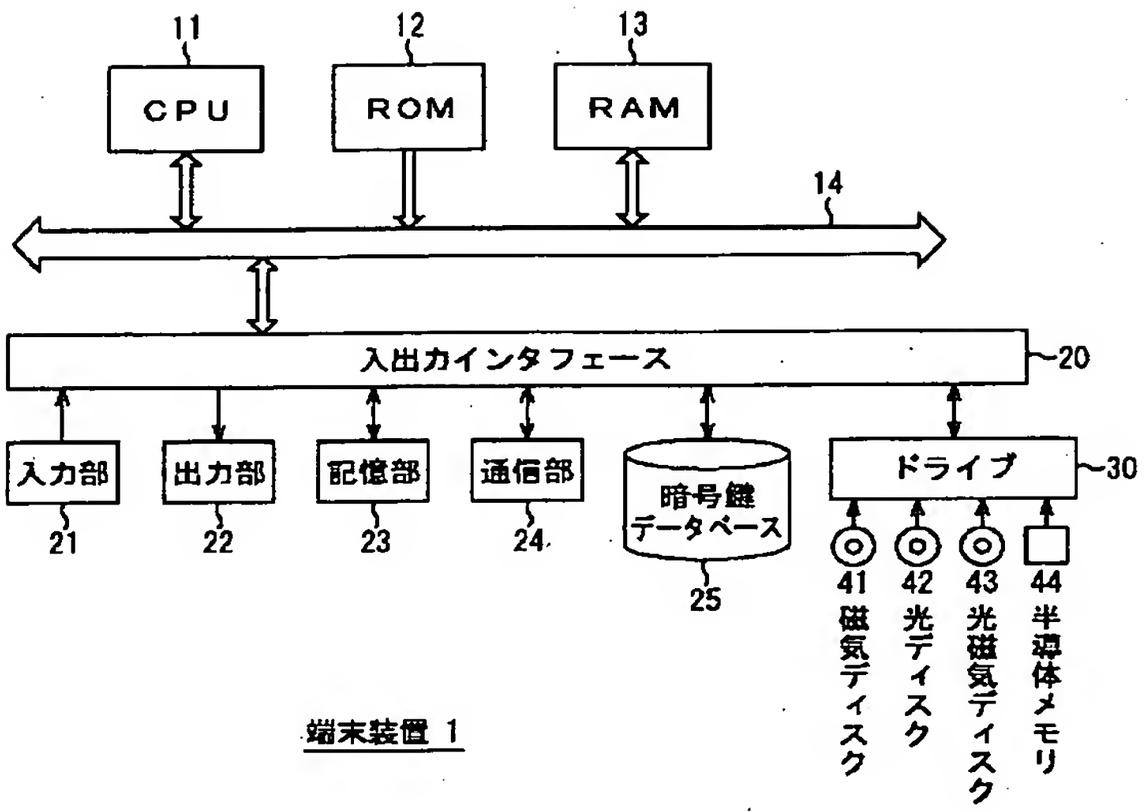

11
12
13
CPU
ROM
RAM
14
入出力インタフェース
20
入力部
出力部
記憶部
通信部
暗号鍵データベース
ドライブ
30
21
22
23
24
25
41 磁気ディスク
42 光ディスク
43 光磁気ディスク
44 半導体メモリ
端末装置 1

図2

【図３】

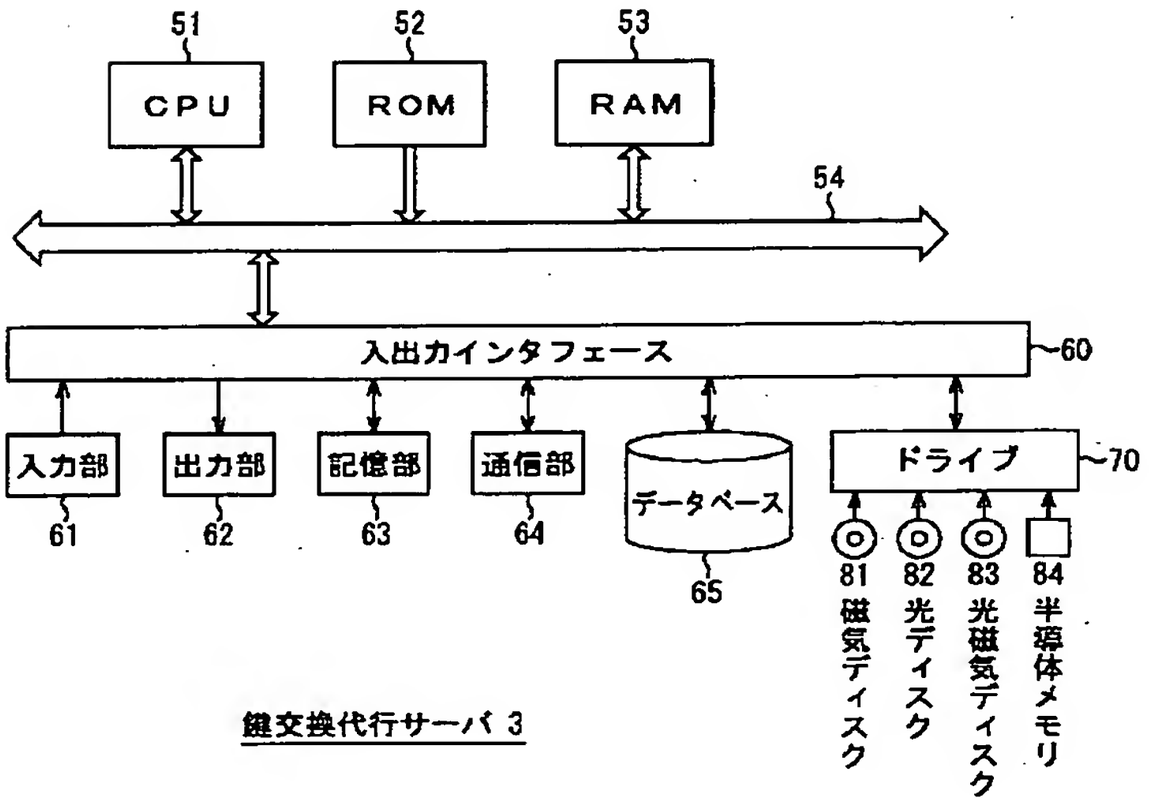
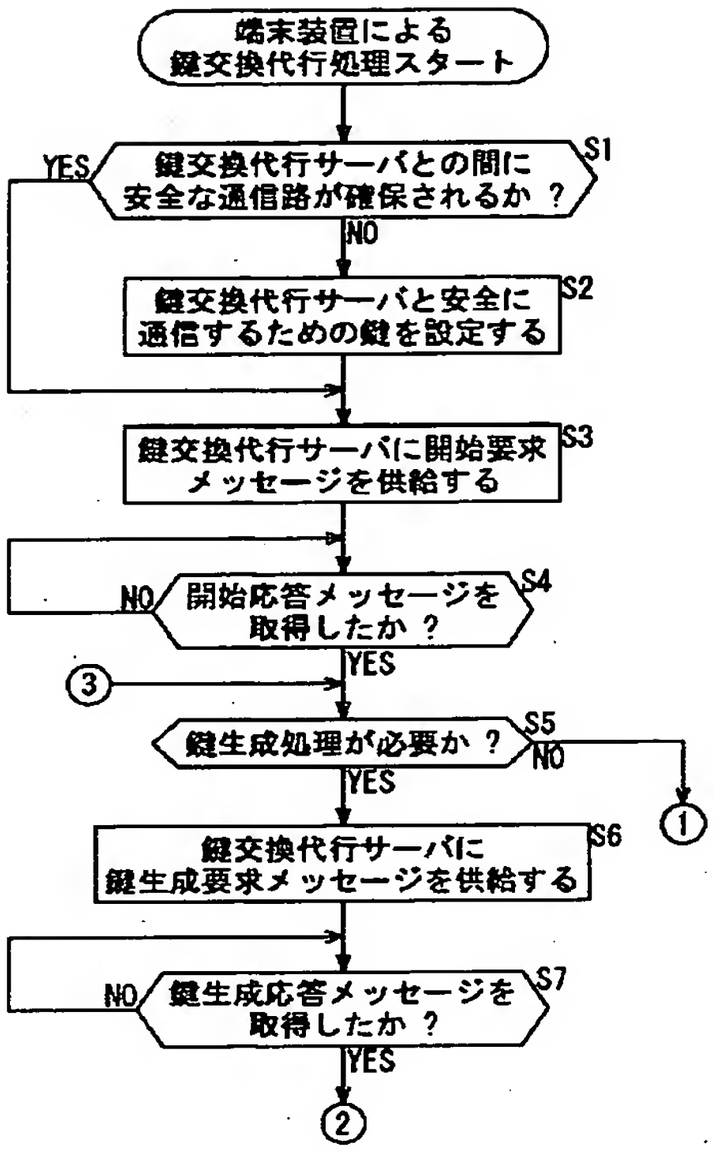

51
52
53
CPU
ROM
RAM
54
入出力インタフェース
60
入力部
出力部
記憶部
通信部
データベース
ドライブ
70
61
62
63
64
65
81 磁気ディスク
82 光ディスク
83 光磁気ディスク
84 半導体メモリ
鍵交換代行サーバ 3

図3

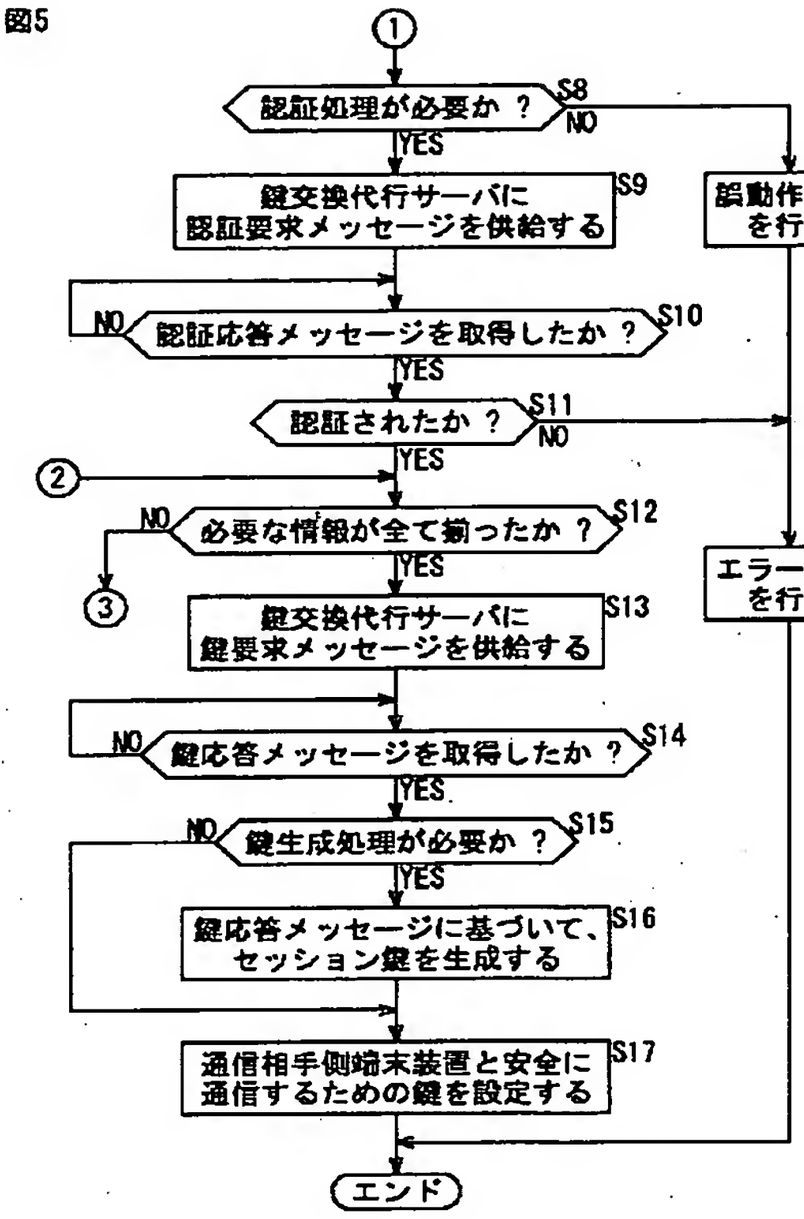
【図４】

図4



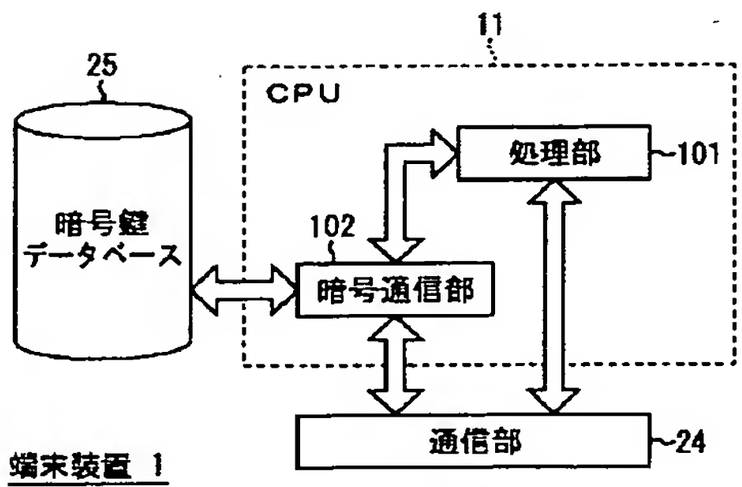
【図５】

図5



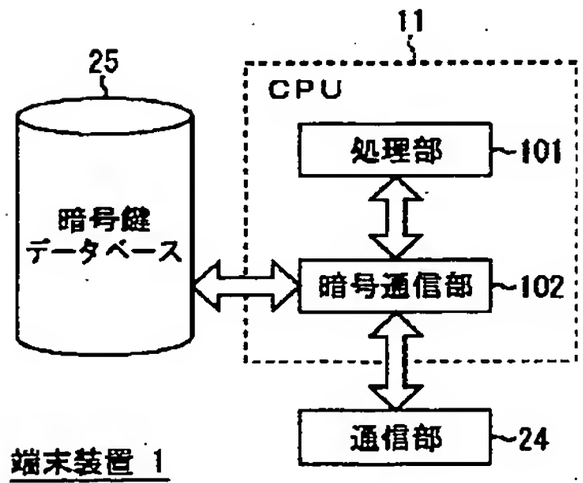
【図６】

図6

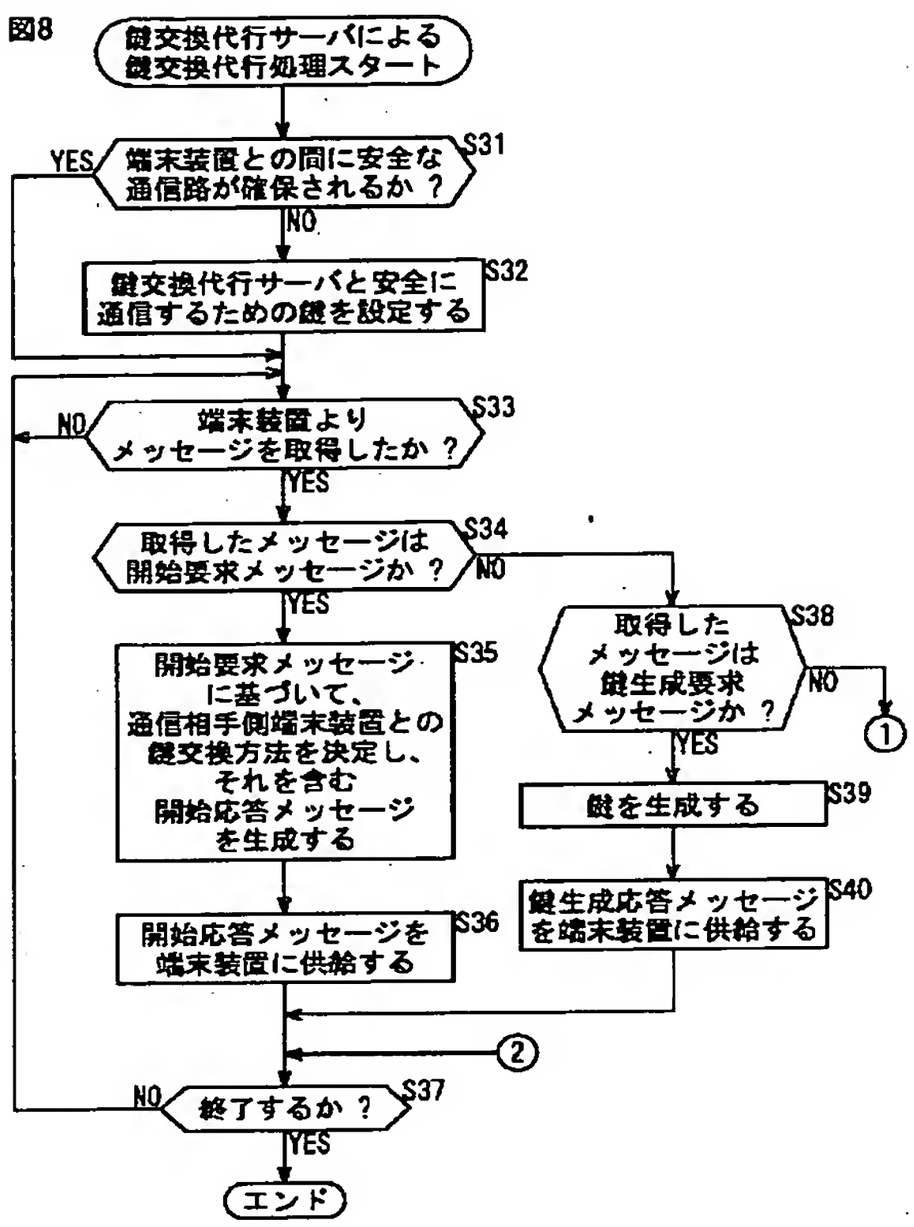


【図７】

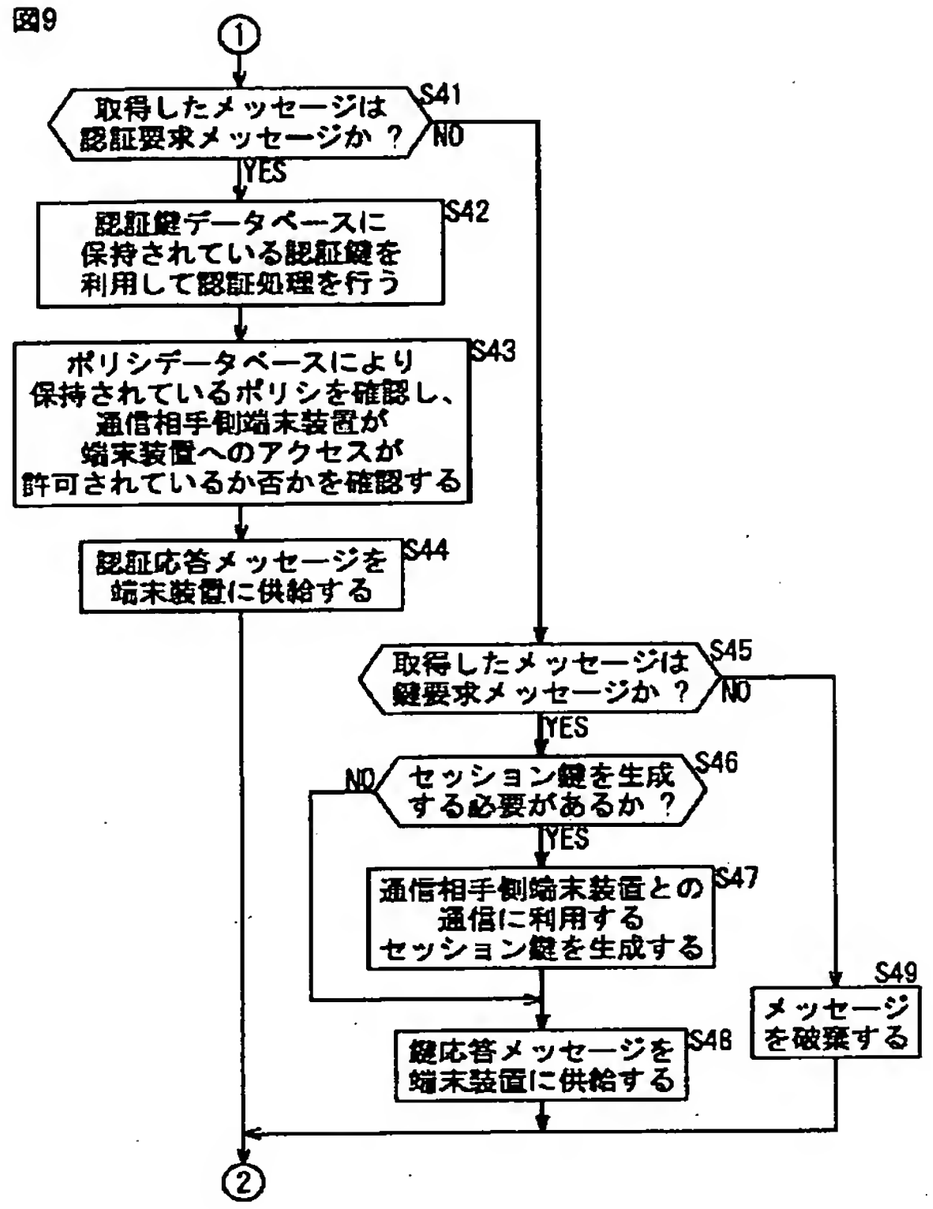
図7



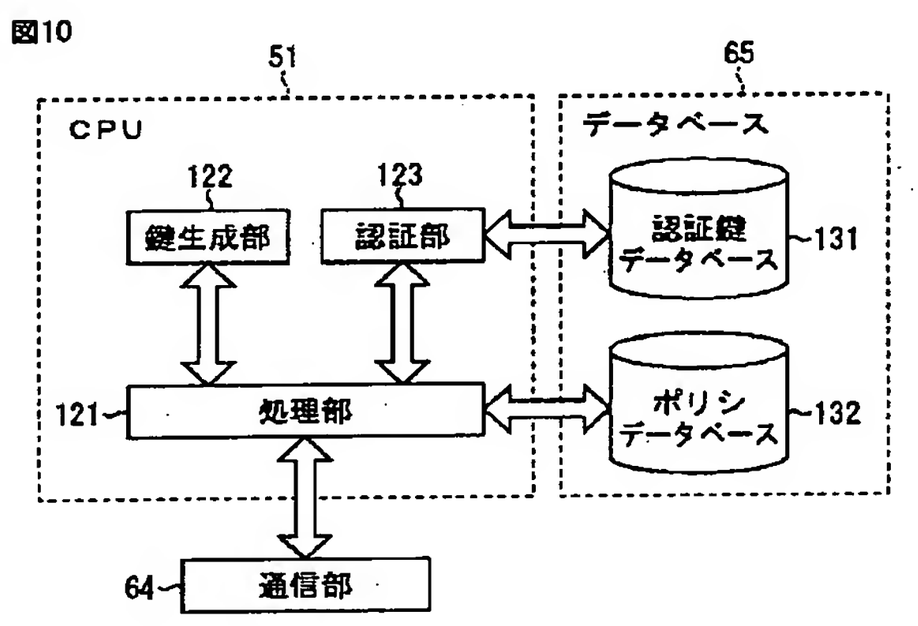
【図８】



【図９】

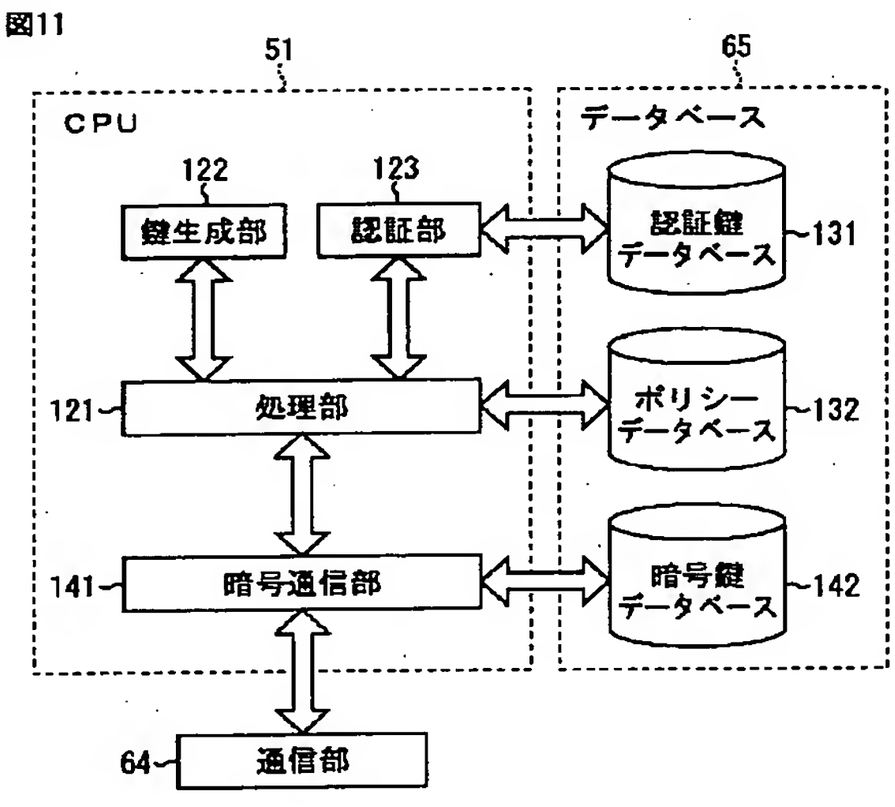


【図１０】



鍵交換代行サーバ３

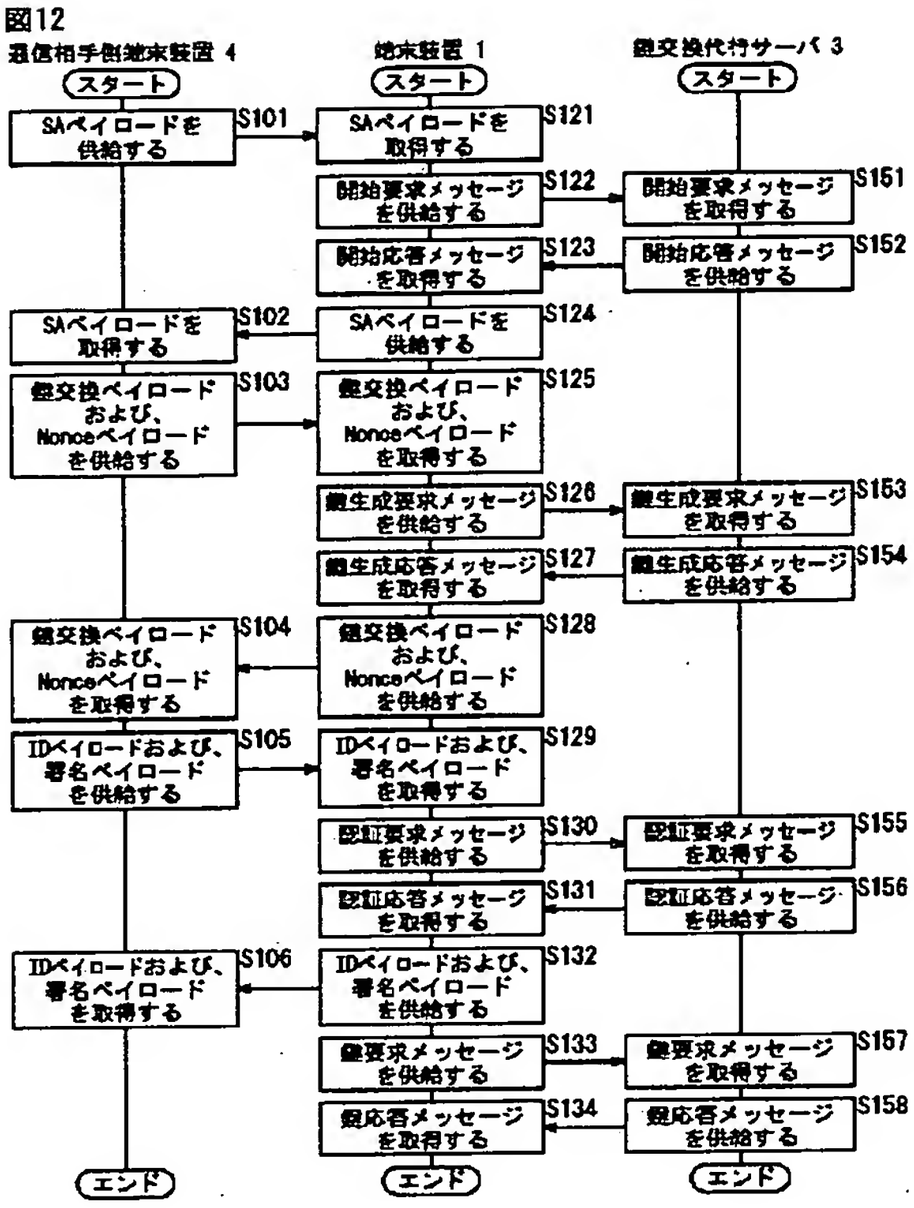
【図１１】



鍵交換代行サーバ３

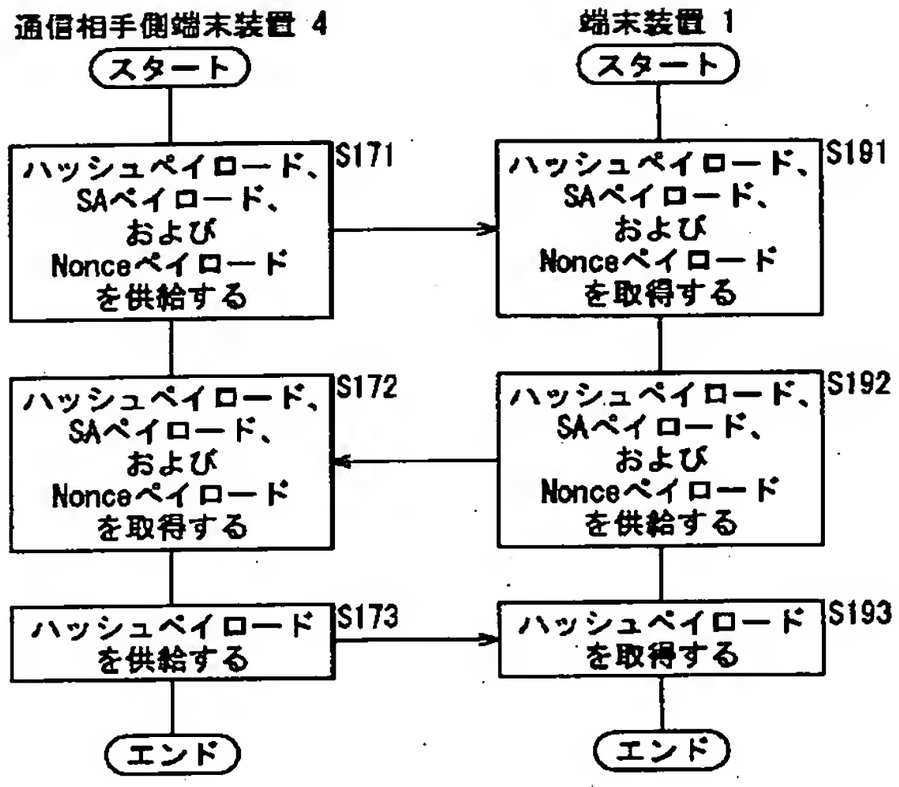
【図１２】

図12



【図１３】

図13



【図１４】

図14